LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR INFORMATIK
Lehr- und Forschungseinheit Medieninformatik

BACHELORARBEIT

Prototyping a Tangible User Interface for Quantum Key Distribution

Timo Weisbarth

Entwurf vom July 12, 2023

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR INFORMATIK
Lehr- und Forschungseinheit Medieninformatik

BACHELORARBEIT

Prototyping a Tangible User Interface for Quantum Key Distribution

Timo Weisbarth

Verantw. Hochschullehrer:	Prof. Dr. Florian Alt
Betreuerin:	Sarah Delgado Rodriguez
Abgabetermin:	12. Juli 2023

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 12. Juli 2023

. . . . . .
(Unterschrift des Kandidaten)

Zusammenfassung

Die sich abzeichnende Gefahr, dass Quantencomputer in wenigen Jahren etablierte Schlüsselaustauschalgorithmen wie den Diffie-Hellman-Schlüsselaustausch brechen könnten, erfordert neue kryptografische Sicherheitsmaßnahmen, um den Fortbestand des Internets, wie wir es heute kennen, zu gewährleisten. Da die Quantenmechanik das Mittel für diese Umbruch in der Technologie ist, könnte sie auch eine Lösung für diese Bedrohung bieten. Einer der potenziellen Kandidaten für die Ablösung des etablierten Diffie-Hellman-Schlüsselaustauschs könnte daher ein Schlüsselaustauschalgorithmus sein, der selbst die Prinzipien der Quantenmechanik nutzt, um wieder die Sicherheit zu gewährleisten. Die Grundlage der meisten modernen Quanten-Schlüsselaustauschalgorithmen ist der BB84-Algorithmus [1]. Es ist also wichtig, ihn als Grundlage für das gesamte Konzept zu verstehen. Während es jedoch für die meisten Menschen bereits schwierig ist, die Grundlagen der klassischen Kryptografie zu verstehen, stellt die Einführung der Quantenmechanik eine ganz neue Herausforderung dar. Um dieses schwierige Thema greifbarer zu machen, hat Linus Stetter in seiner früheren Arbeit [2] einige Ideen für ein Gerät entwickelt, das die Schlüsselkonzepte des Quantenschlüsseltausches spielerisch erklärt. Darauf aufbauend soll in dieser Arbeit nun der erste Prototyp eines solchen Geräts gebaut und getestet werden, ob er in der Lage ist das Thema leichter zugänglich zu machen. Der Bauprozess umfasste eine Vielzahl von Disziplinen wie 3D-Design und 3D-Druck, Elektronikdesign und Leiterplattenherstellung sowie digitale und analoge Eingabeverarbeitung und UI/UX-Design, alles mit dem Ziel, ein Gerät zu bauen, das einfach zu bedienen ist und dessen Bedienung sich gleichzeitig gut anfühlt. Am Ende wurde der fertige Prototyp mit einigen Freiwilligen getestet und es wurden weitere Verbesserungsmöglichkeiten identifiziert.

Abstract

The looming thread of quantum computers breaking established key exchange algorithms like Diffie-Hellman key exchange in just a few years require a new set of cryptographic security measures to be taken in order to ensure the continued existence of the internet as we know it today. Since quantum mechanics provides the means for this disruption of technology, it might also provide a solution to this threat. Which is why one of the potential candidates to replace the established Diffie-Hellman key exchange may be a key exchange algorithm which itself leverage the principles of quantum mechanics to ensure the security of the key exchange. The foundation of most modern quantum key exchange algorithms is the BB84 algorithm [1]. So it is important to understand it as the basis for the entire concept. However while it is already difficult for most people to grasp the basics of classical cryptography, introducing quantum mechanics on top provides a whole new layer of challenges. In order to provide a more tangible approach to this difficult topic, the previous work by Linus Stetter [2] brainstormed some ideas for a device that playfully explains the key concepts of quantum key distribution. Building on top of his work, this

thesis now seeks to build the first prototype of such a device and test if it makes the topic more approachable. The build process involved a multitude of disciplines such as 3D-design and 3D-printing, electronics design and PCB fabrication as well as digital and analog input processing and UI/UX design, all in order to put together a device which is easy to use and at the same time feels good to use. In the end the completed prototype was tested with a few volunteers and further areas of improvement are identified.

Aufgabenstellung

Concepts of IT security are often very abstract, and many persons have problems understanding them or have wrong mental models about them. Tangible User Interfaces (TUIs, i.e., objects that can be manipulated with the hands and enable interaction with digital data/services) have already shown in other application areas that they can help people to better understand abstract processes. The question arises, whether TUI can also support the understanding of abstract IT security concepts, using the example of quantum key distribution (QKD). For this purpose, we have derived design concepts for such a TUI in a previous Bachelor-Thesis.

Hence, the aim of this thesis is the implementation and evaluation of a TUI for explaining QKD (i.e., the protocol BB84) to layman. Concrete tasks would be:

- derivation of requirements and scope of the TUI based on the results of a previously conducted Bachelor Thesis
- design and implementation of the TUI
- evaluation of the TUI through a user study

Contents

1. Introduction

Being able to send secure messages over the internet represents the back bone of many applications nowadays and services like online banking would be impossible without it. For a message to be sent securely it has to be encrypted and the cornerstone of modern cryptography is the secure exchange of a common key for said encryption. However, the increasing power of quantum computers [3] poses a significant risk to how we securely exchange these keys today as they can break the commonly used security measures during the key exchange. Namely these measures depend on so-called one way functions (mathematical functions which are easy to compute in one direction but extremely difficult to reverse) which fore example take two large, prime numbers and multiply them. The multiplication is easily done, but factorizing the resulting number takes in the order of years and is therefore not a feasible attack vector to break cryptography [4]. That is unless a sufficiently powerful quantum computer comes along, since these would be able to solve the factorization problem in the order of minutes instead of years.

Therefore quantum safe encryption is needed in the near future. With most modern symmetrical encryption methods like AES-256 still being considered safe, even with the advent of powerful quantum computers [5], it is mostly the key exchange which must be adapted to a post quantum computer world. Since quantum mechanics provides the means to break the current key exchange standards, the natural conclusion would be to assume that quantum mechanics could also provide the means to ensure the safety of key exchanges again. This assumption has been proven correct by the introduction of the BB84 quantum key exchange algorithm [1]. This algorithm, in conjunction with a true single photon source provides an unbreakable key exchange mechanism, even when faced with quantum computers [6]. Because the BB84 algorithm is still the foundation of even more modern quantum key exchange algorithms [7], it is important that not only IT security experts understand its inner workings and significance. At least on a surface level it is also relevant that policy makers have to at least grasp the fundamentals of this new and emergent technology and why it's important to the security of all online communications. Otherwise it's impossible for them to create informed and helpful policies and laws governing IT security, just like we just now saw with the EU regulations on cryptography [8].

Unfortunately this is quite a tall task since quantum key exchange adds on top of the already complicated field of advanced cryptography the even less accessible field of quantum mechanics. This, in turn, calls for a way to more easily present the algorithm and its concepts in the form of a tangible user interface, capable of explaining these complex relationships in a more accessible manner.

Building on top of the work done by Linus Stetter in his bachelor thesis [2] where he explored different concepts for such a tangible user interface, it is this thesis' goal to create the first practical prototype. Besides refining the ideas of Linus Stetter and the work group into a device with guaranteed reproducibility and audio-visual-cues that convey both the core of the algorithm, as well as the basics of the quantum processes, in

a pleasant, non-intimidating way.

To achieve this, this thesis first dives into the background of both cryptography and quantum mechanics, as well as some material science about what materials humans like to interact with in a tactile way. After that follows a brief chapter about the early design process for the prototype and the results from discussing the resulting design choices with two experts in the field of cryptography and physics to further refine the concepts. Then this thesis will discuss in depth the practical designs and builds and how certain aspects needed quite a few iterations before making it into the final prototype. This deep dive will cover all the relevant parts of the prototype, from the box to the mechanics and engineering, the electronics and finally the software which not only brings all previous parts together but also presents them in a nice GUI. Finally the prototype will be presented to a few people who are not experts in the field of cryptography and their feedback will be used to compile a list of recommendations for further improving the prototype into a fully viable device that allows field experts to share their knowledge with laymen in a fun and educational manner.

2. Related Work

Due to the vast range of topics that this thesis covers, the related work comes from all kinds of disciplines. First and foremost is the previous bachelor thesis that this work is based on. It laid the ground work by crowd sourcing ideas for a tangible user interface for the B84 algorithm. This algorithm itself is part cryptography, part quantum mechanics, so a background in both is advantageous. Of course the tangibility aspect of the interface is a whole field of research in itself and cover the whole range from material science to human psychology. Finally the prototype utilizes a lot of sensors and electronics to capture the users action and a graphical user interface (GUI) to bring it all together.

2.1. The Previous Bachelor Thesis

As mentioned before, the previous bachelor thesis by Linus Stetter [2] did a user study in the form of a workshop to come up with multiple proof of concept models. These models represent the foundation for the design of the prototype that this thesis covers. Before diving into the user study however an extensive deep dive was done on existing tangible user interfaces (TUIs), the materials they used and the interactions with the users. Especially how the different kinds of inputs and outputs require a fluid transition from analog to digital and back.

It's thanks to his in depth analysis of these topics that this thesis can focus primarily on the development of the prototype and the challenges that came with it after establishing only a few of the core principles in the background chapter (chapter 3).

2.2. Cryptography

Since the BB84 algorithm is a (quantum) key exchange algorithm, it's important to understand how the key exchange is handled today and how cryptography in general works, by leveraging both symmetric and asymmetric encryption. To this end the book "Serious Cryptography" by Jean-Philippe Aumasson [9] offers a good yet uncomplicated introduction to all these concepts, covers the important AES cypher and even has a small dip into quantum cryptography at the end. For a more detailed and serious approach that also goes into the mathematics involved, see "Introduction to Cryptography" by Hans Delfs and Helmut Knebl [10].

2.3. Quantum Mechanics

A long standing staple in teaching quantum mechanics is "Introduction to Quantum Mechanics" by David J. Griffiths and Darrell F. Schroeter [11]. This book covers all fundamentals of quantumechanics, the underlying mathematics and pratical applications of both. It is however a bit on the heavier side. For just a brief introduction to the parts

of quantum mechanics, that are important to the BB84 algorithm - namely superposition, polarization and the no-cloning theorem - the two page article "The no-cloning theorem" by William K. Wootters and Wojciech H. Zurek [12] is a good start.

2.4. BB84 Algorithm

The BB84 algorithm is at the heart of this thesis and the prototype which seeks to give a human centered introduction to the core concepts of this algorithm. A more detailed explanation can be found in the original paper "Quantum cryptography: Public key distribution and coin tossing" by Charles H. Bennett and Gilles Brassard after whom the algorithm was named [1].

2.5. Tangibility

A comprehensive paper on the importance of tangibility is "Tangible User Interfaces: Past, Present, and Future Directions" by Orit Shaer and Eva Hornecker. It describes how TUIs bridge the gap between the physical and the digital world, by enabling more intuitive and engaging interactions, supporting cognitive processes and fostering collaboration and social interaction [13].

2.6. Electronics

A comprehensive guide to all things electronics can be found in the books by P. Horowitz and W. Hill. Their textbook "The Art of Electronics" gives a very detailed theoretical background into electronics and electricity [14]. The compendium book "The Art of Electronics: The x Chapters" provides an excellent reference resource for real world applications of the theoretical systems introduced by the first book [15] and even provides circuit designs with partn umbers for easy replication of even complex systems.

The Rapsberry Pi has an introductory book called "Getting Started with Raspberry Pi" by Matt Richardson and Shawn Wallace [16]. This book covers the basics and explains how the programming language python can be used to utilize the GPIO ports of the Raspberry Pi. Additionally the chapter about the Pi and Arduinos is useful for connecting the Raspberry Pi and the Raspberry Pi Pico.

3. Background and Theory

The main focus on this project is the accessibility to complicated and at times difficult to understand concepts from the fields of cryptography and quantum mechanics. In order to evaluate which of these areas are key concepts and need to be represented in one way or another in the final product, it is important to understand the underlying, theoretical background.

In this chapter we will take a look at the aforementioned theoretical background and introduce the core concepts of cryptography and quantum mechanics. The cryptography part will focus on how computer cryptography works today, using symmetric and asymmetric encryption to provide both plain text enciphering and remote party authentication, as well as key exchange. The part about quantum mechanics will provide insights into polarization and superposition of states and how cryptography can be improved upon by utilizing these mechanics.

3.1. Cryptography and Key Exchange

The goals of cryptography are generally considered to be to provide data integrity, authentication and non-reduplication [10].

Data integrity	Ensure the data has not been modified in transit. This covers both intentional and accidental modification.
Authentication	Ensure the sender of the message is actually who they claim to be.
Non-repudiation	Ensure the ownership of the message so that the writer can't later deny writing it.

To achieve these goals a combination of symmetrical and asymmetrical cryptography is needed which the following sections will go into greater detail about.

3.1.1. Symmetric Encryption

Symmetric encryption is a fairly simple concept to grasp: it relies on a secret key which both parties involved know, but which is unknown to any third party. Lets call the two parties that want to exchange an encrypted message Alice and Bob. With both of them in possession of a common secret key, either one is able to send the other a secret message by interposing the message with the key [17]. This condition - to have to use a secret key - is one of the main flaws of symmetric encryption, as opposed to asymmetric encryption, where a known key is used - a so-called public key [18].

3.1.2. Asymmetric Encryption

Asymmetric encryption or public-key cryptography is a system of encryption where a pair of related keys is used: a public key and an associated private key, whereby the public key enables one to encrypt a message, resulting in ciphertext, which can then be decrypted exclusively by someone who knows the associated private key, in order to understand the initial message [19]. Cryptographic algorithms generate key pairs using mathematical instances known as one-way functions. In public-key cryptography, the security relies on maintaining the secrecy of the private key, while the public key can be openly shared without jeopardizing the security [20].

3.1.3. Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange is a mathematical technique, where cryptographic keys are safely being exchanged over a public channel. It is considered one of the pioneering public-key protocols in the field of cryptography. The method was conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman and is one of the earliest practical implementations of public key exchange. Published in 1976 by Diffie and Hellman, their work first introduced the concept of a private key and the public key associated with it [21].

3.2. Quantum Mechanics

With quantum mechanics being at the core of the BB84 algorithm, at least a basic understanding of it is necessary to grasp the algorithm itself.

The foundational work on QM regarded the behavior of small particles like electrons, α-Particles or photons. Their behavior is described by the partial differential equations known as the Schrödinger-Equation.

$$-\frac{\hbar^2}{2m}\Delta\psi(\vec{x},t) + V(\vec{x},t)\psi(\vec{x},t) = i\hbar\frac{\partial}{\partial t}\psi(\vec{x},t) \tag{3.1}$$

Without going into too much detail about every part that makes up the Schrödinger-Equation, it is only important to understand, that its solutions are wave functions, but these solutions do not describe a wave-like behavior of a medium but the probability of particles being at a spot. This was observed in the double slit experiment where particles were sent through two slits and created light dots on a screen afterwards. Given enough time and enough particles the probability of finding a light dot on the screen at any point wasn't what is expected from naively assume ball like particles, meaning the sum of two Gaussian curves, but an interference pattern that would be expected of waves. Meaning individually sent particles passing through a double slit express wave-like behavior regarding their probability of appearing at any point after the double slit.

Other important concepts of quantum mechanics are the so-called no cloning theorem which states that it is impossible to create an identical and independent copy of an arbitrary unknown quantum state. In other words, one cannot clone an unknown quantum state perfectly. This fundamental principle arises due to the nature of quantum superposition and the measurement process, which results in the collapse of the state upon observation. Said collapse being the wave function, which is the solution to the

Schrödinger-Equation no longer being a probability wave, but collapsing into absolute certainty (within the limits of the Heisenberg uncertainty principle of course) [11]

3.2.1. BB84 Algorithm

The BB84 algorithm relies on the principles described in the previous section on quantum mechanics to allow for a provably secure exchange of a cryptographic key. It works by sending single photons from a sender called Alice to a receiver called Bob. While sending a photon Alice chooses randomly if she sends a 0 or a 1. Additionally she chooses a random encoding base for the photon, which can be either orthogonal or diagonal polarization. Bob now receives the photon and also randomly chooses a measurement base for the photon. As a result of the measurement Bob either measures a 0 or a 1.

Once Alice has sent a sufficient amount of photons the two will exchange the bases they used for each photon over a public channel. Now they can compare where they randomly chose the same base and use the resulting bits for a key. The equality of the bases is important, because differing bases mean, that Bob will have measured either a 0 or a 1 with equal chance, regardless of what Alice actually sent.

The now generated key must still be verified, because an eavesdropper in the middle could have made their own measurements. This interception however is easily detectable by Alice and Bob, through simply exchanging the first 10% of the key they just generated. If the key fragments match, then depending on the key length, it is unlikely that an eavesdropper was present. If the key fragments however differ, then the presence of an eavesdropper is almost assured [1]

3.3. Tangible User Interfaces

Tangible user interfaces (TUIs) refer to interfaces that enable interaction between users and digital information through physical objects. These interfaces aim to bridge the gap between the physical world and digital information by incorporating physicality and tangibility into the user interaction. TUIs often involve the use of physical objects or artifacts that can be manipulated, sensed, or recognized by a computer system. These objects serve as tangible representations or controls for digital information or actions. By manipulating these physical objects, users can interact with and manipulate digital data in a more intuitive and natural way [22].

The concept of TUIs emphasizes the importance of the physical and sensorial aspects of human-computer interaction. It suggests that incorporating physical objects and physical actions into the interface design can enhance user engagement, understanding, and creativity.

Overall, tangible user interfaces aim to create more seamless and embodied interactions between people, digital bits, and physical atoms, allowing users to manipulate and interact with digital information using their physical senses and cognitive abilities.

3.3.1. Why Tangibility is Important

The significance of TUIs, or rather of physicality, tangibility, and embodied interaction in TUI design can be seen in various aspects associated with these concepts [13]:

- Bridging the physical-digital divide: TUIs aim to bridge the gap between the physical and digital worlds by providing users with tangible objects that can be directly manipulated. This physicality enables a more natural and intuitive interaction, allowing users to leverage their existing physical skills and cognitive abilities.
- Enhancing engagement and understanding: Physicality and tangibility in TUI design can enhance user engagement and understanding. By incorporating physical objects and manipulations, TUIs provide a more sensory-rich and immersive experience, allowing users to form a stronger connection with the digital information or system being represented.
- Supporting cognitive processes: TUIs leverage the embodied nature of interaction to support cognitive processes such as learning, problem-solving, and creativity. The physicality and tangibility of TUIs provide users with a tangible representation of abstract concepts, making them more graspable and manipulable. This can facilitate exploration, experimentation, and the development of mental models.
- Expanding interaction modalities: TUIs enable interaction beyond traditional input devices such as keyboards and mice. By incorporating physical objects and gestures, TUIs allow for a wider range of interaction modalities. This can accommodate diverse user preferences, abilities, and cultural practices, fostering inclusivity and accessibility.
- Fostering collaboration and social interaction: TUIs have the potential to facilitate collaboration and social interaction by providing shared physical artifacts that multiple users can manipulate together. This promotes communication, negotiation, and joint problem-solving, creating a more collaborative and social experience.

All in all, TUIs offer unique benefits in terms of naturalness, engagement, cognitive support, expanded interaction modalities, and social interaction and, by aligning themselves with human capabilities, improve the overall user experience.

3.3.2. Choice of Materials

The specific choice of materials for TUIs are dependant on multiple factors, such as design, functionality and user experience. Therefore it cannot be claimed that a universally best material exists, but there are a couple of contenders, based on overarching requirements [23]:

- Plastic: Very versatile, by virtue of being highly moldable, durable, lightweight and is commonly seen in physical objects. Different types can also offer different tactile qualities and aesthetic options.
- Wood: Being a material found in nature, it can bring out a feeling of connection to one's surroundings and with it a tactile feel to the TUI. It is highly malleable as well, since it can be carved, formed and finished in such a way to fabricate not only ergonomic objects, but also visually appealing ones.
- Metal: Materials like aluminum or stainless steel are popular because of their longevity and sturdiness, which is why they can be used to create resilient and enduring components in TUIs. As far as aesthetic is concerned, metal can provide both a modern and industrial aesthetic.

The mentioned materials were also used for the construction of the prototype.

3.3.3. Size Considerations

As described in the bachelor's thesis [2], that this thesis is based on, it is practically impossible to talk about absolute numbers, when it comes to sizes of TUIs, but what can be done is relating them to each other. In this sense, three categories have been formulated: small, medium and large TUIs.

First category represents TUIs that can be operated by a single hand and is exemplified by Beads that create light patterns and Thinking-Tags [24], that exchange information when users are in the vicinity of each other. This can be used, for example, to depict a spread of a virus, by analyzing meta-information the tags gathered.

Second category comprises of TUIs that can "no longer fit into a pocket". An example for this would be a toy-looking caterpillar called TellTale, which can record voices and play them back, with each of the five parts of the caterpillar having a button for this [25].

Third category epitomize the type of TUI to be worked on by a number of people, such as TableTop TUIs, which the prototype is one of.

4. Design

4.1. Early Design Considerations

Being based on a the previous bachelor thesis by L. Stetten [2], the initial design considerations took into consideration the results of this thesis. Since [2] provided two potential solutions the best of both were considered and evaluated for practicability. With the primary takeaway being that a hands on design should be favored and a physical object representing a photon should be exchanged between parties. Although the original thesis suggested a sort of air-hockey table over which users can send chips, this solution was deemed to unreliable. This is where the idea of using a marble track first came in. With a marble track basically the same design patterns as with the air-hockey table can be followed, but in a more controlled and repeatable way. Additionally the design was a bit simplified to make the marble track easier to build, which meant to combine the two gates both the sender and receiver had into a single gate that can be switched from one base to the other through the use of a rotating switch.

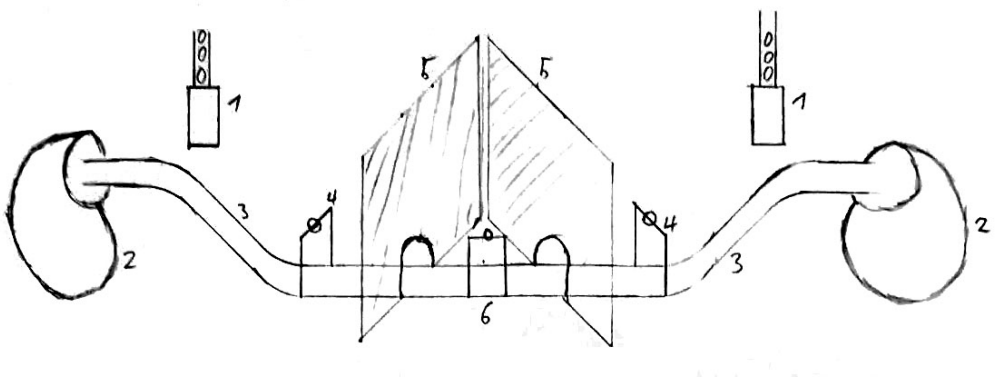

Figure 4.1.: Initial proposal overview, depicting the track and the components needed for exchanging marbles

The result of these considerations can be seen in Fig. 4.1. This first proposal depicts a track (3) which allows two parties to send marbles to each other. A marble dispenser (1) a distance over the sloped part of the track gives the marbles enough velocity to reach the marble catcher (2) on the other side while passing through two gates belonging to Alice and Bob (4) and - depending on whether an eavesdropper is present or not - the gate of Eve (6). The gates each have a rotating button to represent the measurement base and the dispensers allow for a selection of sending a marble representing a 0 or a 1. Independent of the selection made with the dispenser, the marbles would all look the same, since in reality the photons are also indistinguishable until measured by a polarizing filter in a given base. A view cover (5) between each of the parties ensures that everyone can only see their own gate. Details on the design of individual parts can be seen in Fig.

4.2.

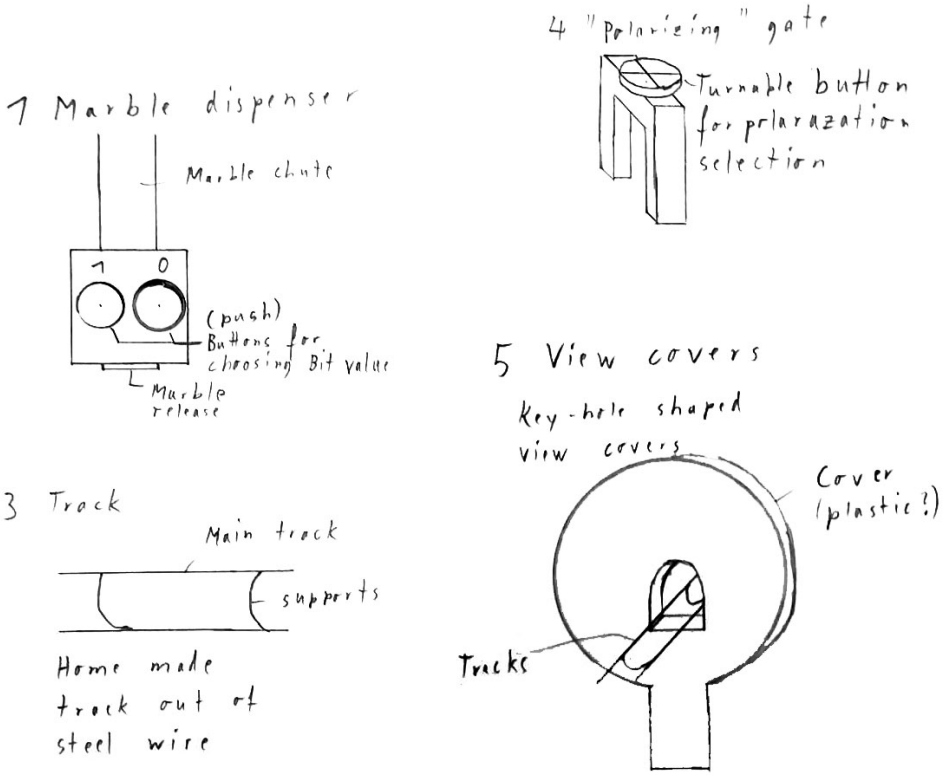

Figure 4.2.: Detail design considerations for specific parts of the initial proposal

The material choice at this time only specified that the track should be made out of steel wire. Steel wire provides a rigid frame upon which other parts can be built and also comes with a pleasing aesthetic. Other materials considered were cloth for the marble catchers, but this was still undecided.

Because the view covers would probably be the largest single object in the entire prototype they play a key role in visually relaying the desired impression of the design. As the prototype should be used to explain a cryptographic algorithm, the quint essential impression should be that of security, which is why a key hole shape was considered at this stage.

4.2. Direction and Choices

At this point the initial design was proposed to Prof. Alt and parts of his team to get an early feedback. Additionally the expert opinion of two cyber security experts with a background in physics was obtained through a video call.

From these exchanges the design was further refined to include the following key points:

- To simplify the design and not overwhelm the users, it was decided to have a dedicated sender (Alice) and a dedicated receiver (Bob) instead of enabling them both to send and receive.
- To give a better feeling for the differences in the initial polarization of the photons, the dispenser should release the marbles to either side, depending on whether a 0 or a 1 was dispensed. Afterwards they should be joined before reaching the gate of Alice and then travel down a single track to Bob to represent the indistinguishableness once they leave the are of Alice.
- Similarly Bob should have a split in his end of the track, which divides the marbles up into left and right, again representing a 0 and a 1. Of course his divider has to base the distinction on the measurements taken by Bob, which means that a marble being dispensed on the right side on Alice's end may end up being sorted left on Bob's end.

On top of these changes proposed by the team at the Bundeswehr Universität, it was furthermore decided that both Alice and Bob should get a screen which keeps track of the photons and polarizations for them. The updated design with initial measurements was built in Blender and can be seen in Fig. 4.3. A consideration was made to give Eve also a screen, but since the main purpose of the prototype is to show how measurements taken by an eavesdropper would influence the key received by Bob and not to actually show interception of a key, it was ruled as a practical choice to leave out, since two screens could be handled by a single device.

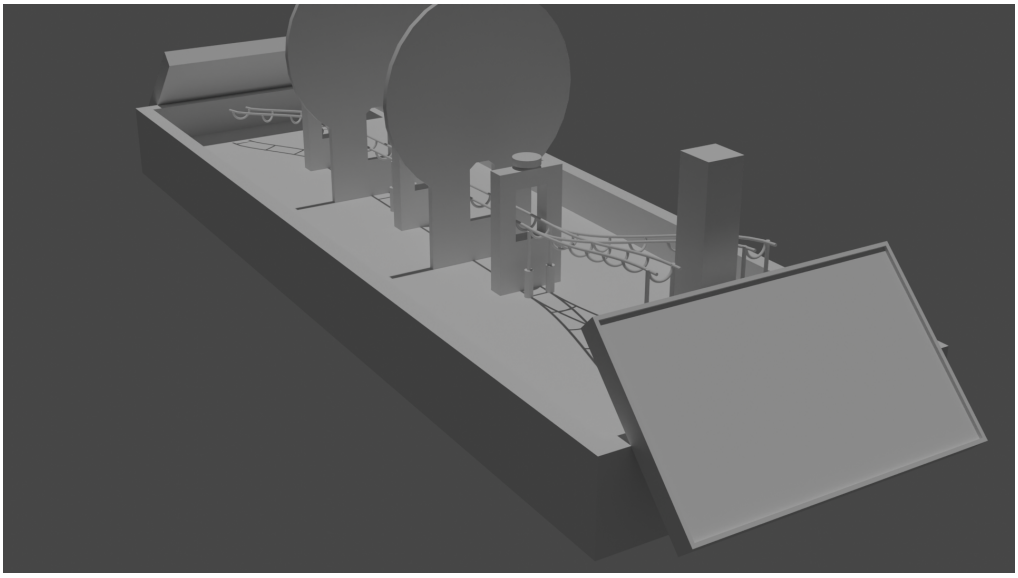

Figure 4.3.: 3D design after finishing the initial design phase

5. Prototype

After the initial design phase was completed, the prototype was being put together. The design was constantly updated to reflect any changes which became necessary in the building phase. Some of these changes were simply made based on what resources were readily available and some arose from challenges encountered.

5.1. The Box

5.1.1. The Base

To hold everything together a proper box was needed. As show in section 3.3.2 it comes quite natural to humans to work with wood, which is why wood was chosen as the basis for the box. Thanks to laser cutters becoming more and more readily available, a good start for the box was found in a site which provides pre-made box designs that can be altered to match custom size requirements [1].

Figure 5.1.: Base model of the "ElectronicsBox" which was adapted for the base box of the prototype [2]

[1] `https://festi.info/boxes.py/`

After deciding on the "ElectonicsBox" [2] for the basic design, shown in in Fig. 5.1, several alterations had to be made. First of all the laser cutter available at the institute was a "MAKEBLOCK LASERBOX PRO" which has a maximum working area of 500 mm × 300 mm which means that the 600 mm long box had to be split into at least two parts. Taking into consideration the available sizes of the wooden slabs (300 mm x 300 mm) and accounting for overhead and the advantages of having multiple parts to be cut on a single slab, the final design split the box into three parts of equal sizes. To increase stability of the complete box, the wall between the outer parts and the inner part was made to be a common wall (instead of having two walls for the individual parts), which was achieved by removing every other teeth from the adjacent walls to allow for a three piece joint instead of the original two piece joint.

Secondly the original design for the box wouldn't provide an inset working area for the marble track which would also double as the mounting frame for the display cases. To account for this the initial floor height was raised and the entire design flipped upside down, which means that the floor is now the top plate on which all other parts, except for the micro controllers and power supply, will be mounted.

For convenience a few more alterations were made. These include two circular holes in the common wall between the outer parts and the inner part to allow for cables to run through the entire box. Also a few cable holes were added to the top plates and holes for the power socket and power button were added to one side panel. To ease laser cutting the entire box was split into seven files, which each fit onto the wooden slabs for batch cutting. The resulting box is shown in Fig. 5.2

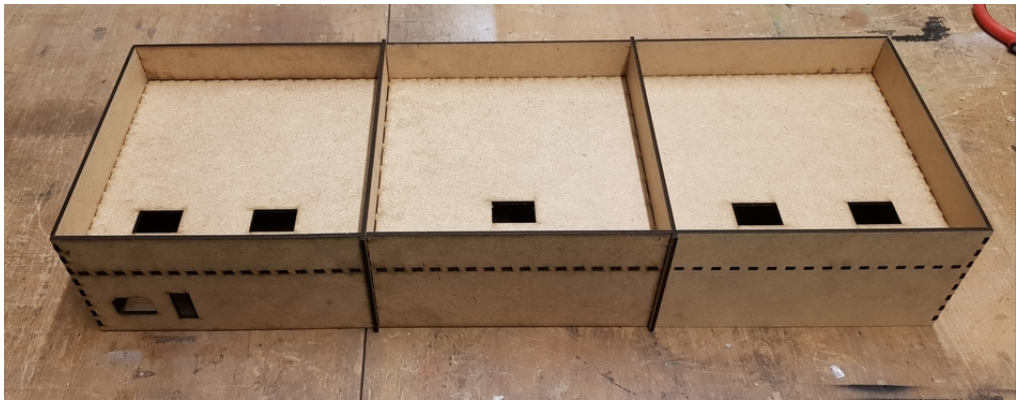

Figure 5.2.: Completed base box for the prototype

Overall the box fit together rather well and the margins were tight enough that it could hold together without applying any glue yet. After this initial testing of the box, it was taken apart once more to add the screw holes for mounting the 3D printed parts (see section 5.3 for details).

5.1.2. Display Case

With the base box completed two mounts for the displays were still required. These were hand designed based on the files for the box and added an extrusion on either side

[2] `https://festi.info/boxes.py/ElectronicsBox`

which will slide right on top of the outer walls of the inset base. This allows for easy attaching and detaching of the display cases whenever needed. The openings on the side line up with the ports on the actual display itself and give access to the HDMI and Micro-USB connectors. The displays are angled at 45° which both provides for a pleasant viewing angle when sitting in front of the box, as well as comfortable access to the on screen buttons which the user will press during the interaction with the prototype. It was considered to have the display cases mirrored since it would have meant that the ports on both displays cases are accessible from the same side. However the asymmetrical shape of the display itself made this more difficult and it was decided that a consistent user experience is more important than having shorter cable routes.

Putting all together results in the completed outer assembly of the prototype as shown in Fig. 5.3

Figure 5.3.: The finished outer assembly of the prototype

5.2. Electronics

With the box done, the rough dimension in place and since most of the 3D-printed parts need to be designed around the sensors they have to host, the next order of business was to design and build the electronics. The first step required was to compile a list of all actions that need to be captured by the electronics and the resulting action performed. This list is compiled into Table 5.1.

We can see that two actions apply to all three users, which means that they each need three sensors. Two sensors are needed to capture the marble release and all outputs to the LEDs need to be transmitted. To bring all the different signals together the choice fell on a Raspberry Pi, as it's a micro computer with an extensive library for GPIO. That of course limited the choices of sensors a little bit, since the Raspberry Pi is only capable of receiving digital signals. To provide everything with power, a power supply and proper on/off switch was also included in the design. Additionally the LED strip which was chosen for the design, required a 5V data line, while the Raspberry Pi is only capable of outputting 3.3V. To amend this a level shift had to be included. The same is

Action	Data to capture	Resulting action
Releasing a marble	Marble release right or left for 0 and 1	Register a photon being sent in Alice's registry. Activate correct LED strip
Rotary dial turned*	New state of the dial (polarization base)	Change color of gate LED to signal polarization change
Marble passes gate*	Photon (marble) measured by the owner of the gate	Capture current state of rotary dial and register it in the registry of the gate owner. Optionally change the direction of the servo motor

Table 5.1.: All actions and the signals that need to be captured and sent by the electronics
*can be applied to either Alice, Bob or Eve

true for the IR LEDs which is why an additional bi-polar NPN transistor was added for each IR LED.

5.2.1. Version One

With this information the first design for the electrical hardware was completed. It is shown in Fig. 5.4 and contains the parts in table A.1 in the appendix. All circuit designs were done in KiCAD, an open source electrical CAD program.

Some of the parts are note immediately placed in the circuit diagram, like the connectors and socket boards, since they are meant to connect the pins of different components together. The circuit has the Raspberry Pi in the center as the central data entry and output point. To the left are the three IR LEDs and their respective sensors together and the necessary level shifting transistors and limiter resistors. To the right is the level shift with outputs to all programmable LEDs.

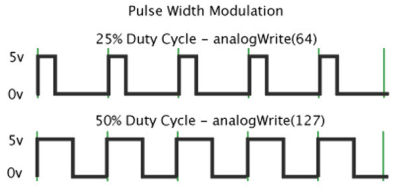

Figure 5.5.: Example PWM signal [26]

While this circuit does not yet contain all the required components to capture every signal (for example the rotary dials are missing), it already provided a solid basis for testing and making sure that every thing worked as intended before expanding the circuit and finally sending it off to have a PCB manufactured. During the testing of this setup is was found to contain some significant flaws. At the center of these issues are the PWM capabilities of the Rapsberry Pi. PWM stands for Pulse Width Modulation and describes a digital signal with a set frequency and a variable on- and off-time during each cycle. For example a 50%, 50 Hz PWM signal will always have a period of 50 Hz and be high 50% of the time and low 50% of the time. In contrast a 25% 50 Hz PWM signal still has a period of 50 Hz but only be high 25% of the time and low 75% of the time. An example of this can be seen in Fig. 5.5. The issue now is that the Raspberry Pi has two PWM channels but the library of the programmable LEDs (rpi_ws281x) takes both channels and doesn't leave a second one for the IR LEDs

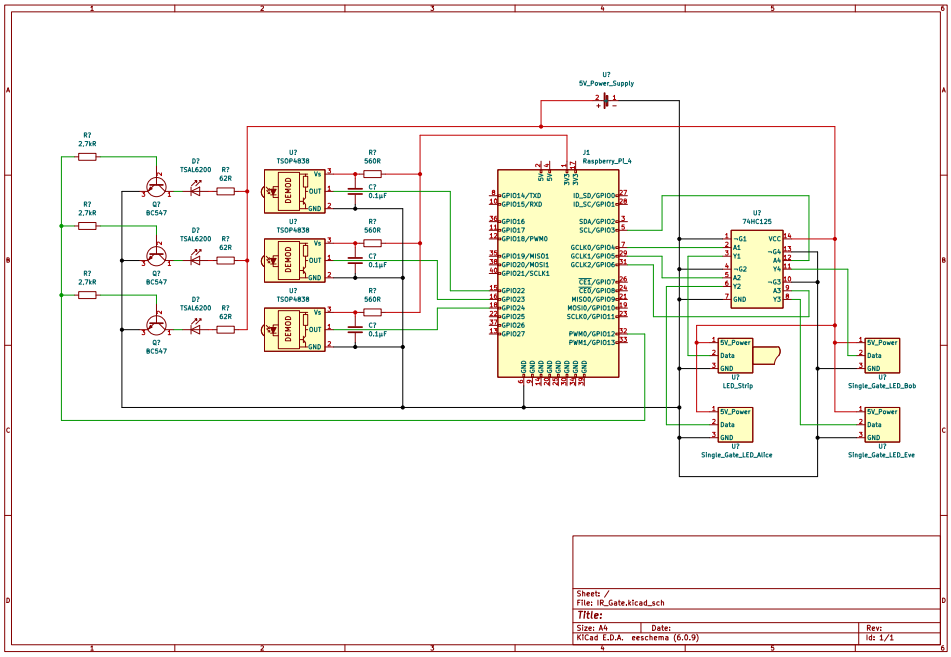

Figure 5.4.: First design of the electric circuit

which have to be switched at exactly 38 kHz for the IR sensor to register them. This feature was originally chosen to make the sensors more resilient to other IR sources, but now is hindering the progress of the project.

With the rpi_ws281x library requiring a speed of 800 kHz to write the programmable LEDs (a clock that is set in hardware on the LEDs themselves) a software PWM signal was also not a viable option. On the other hand, the servo only needs a 50 Hz PWM signal, which the software PWM of the Raspberry Pi can easily provide. After a few more tries to unbind one of the PWM channels from the rpi_ws281x library it was decided that a constant 38 kHz signal source was the easier route to go, which lead to version two.

5.2.2. Version Two

To satisfy the need for a constant 38 kHz source a few options were considered. The issue could have been solved with a simple quartz at the right frequency, however there would have been some overhead involved in redesigning a circuit that adequately supplies the quartz with power and without an oscilloscope readily available, debugging in case something went wrong would have been difficult. Around this time there were also some problems emerging with the design of the rotary dial (see section 5.3.1 for details), which were used for setting the polarization of the gates, and an opportunity was seen to solve both issues at once with the incorporation of a proper micro controller into the setup. Since the Raspberry Pi cooperates well with the micro controller Raspberry Pi Pico and said micro controller was inexpensively available, the choice fell on it.

With the Raspberry Pi Pico in the setup it was now possible to process analog data

as well as digital data. So the rotary dials were switched from a digital, electrical switch button to a potentiometer which could encode every rotational setting. The Pi Pico then processes this analog signal from each of the three dials and forwards a digital signal to the Raspberry Pi. Additionally one of the many PWM channels of the Pi Pico was set to 38 kHz and provided a designated source for the IR LEDs. The redesigned circuit can be seen in Fig. 5.6 and the additional parts, that were needed are listed in table A.2 in the appendix.

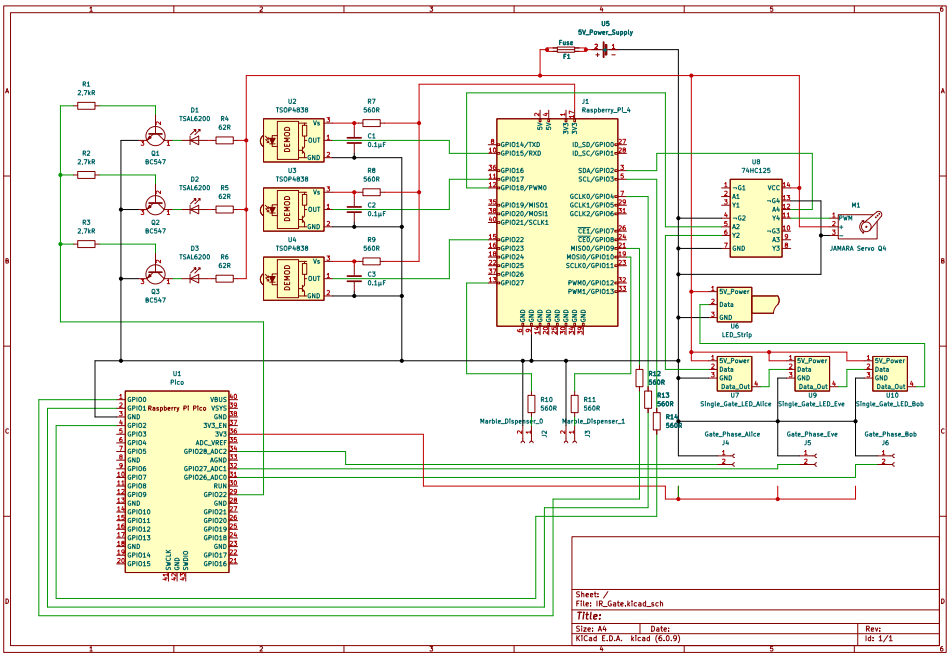

Figure 5.6.: Second design of the electric circuit

The most significant changes in this version - besides the addition of the Pi Pico - are the integration of the servo motor and the rearrangement of the programmable LEDs to be controlled by a single PWM output from the Raspberry Pi. The choice to utilize only the second and fourth latch of the 74HC125 level shift was made purely out of necessity: the first latch of the delivered unit arrived broken and was unusable.

Since there was now a significant load in the system, seeing as the theoretical maximum power draw of all LEDs could be around 5A, the servo could draw another 1A and the Raspberry Pi has a potential peak power consumption of 2.6A, this now could hypothetically draw more ampere than the power supply could provide. Which is why a 8A fuse was also included in this design.

5.2.3. PCB

With the completion of the circuit diagram it was now time to design a PCB which would act as a sort of breakout board for the Raspberry Pi and allow for the connection of all sensors, the LEDs and the servo through proper plugs instead of plugging them in directly into the GPIO pins of the Raspberry Pi.

Thanks to custom made connectors which combined some inputs and outputs onto the same plug, like the two pins for the IR LEDs and the two pins of the dial input coming from the Pi Pico, it was possible to effectively only use two different types of plugs: a four pin connector for most individual components and a twelve pin connector for the Raspberry Pi itself. The resulting two layer PCB design can be seen in Fig. 5.7

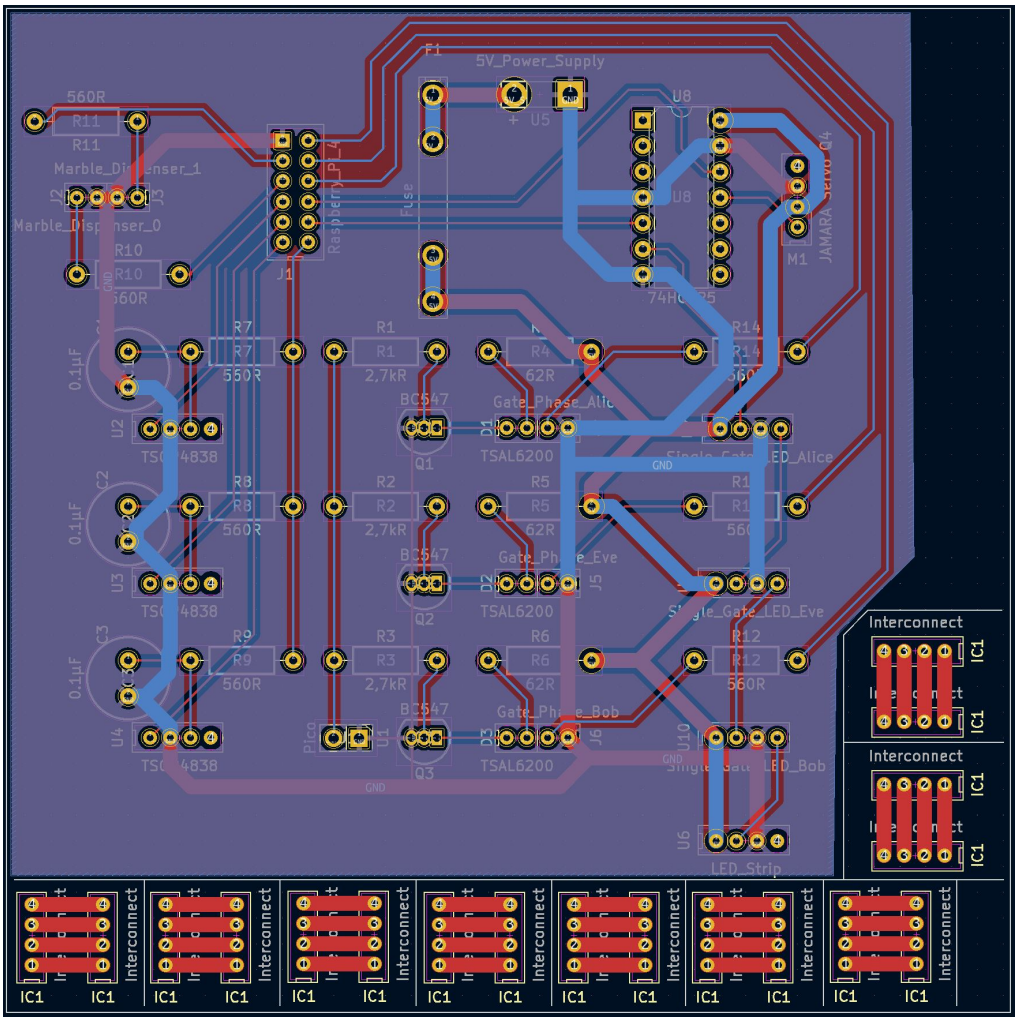

Figure 5.7.: Final PCB design, ready to be manufactured

Of course as is standard the two ground circuits on either side were turned into ground planes that span the entire board and should help with interference. The "Interconnects" which are visible around the lower edge of the board were a planned feature, but the manufacturer said that they could not be cut out in the way the design required, which is why they were ultimately not used.

With everything in place the design was sent off to be manufactured. After clarifying with the manufacturer that the aforementioned feature was not possible they printed it with a standard rectangular cutout resulting in the boards shown in Fig. 5.8.

The overall manufacturing quality was satisfying and no immediate issues were found when testing the board.

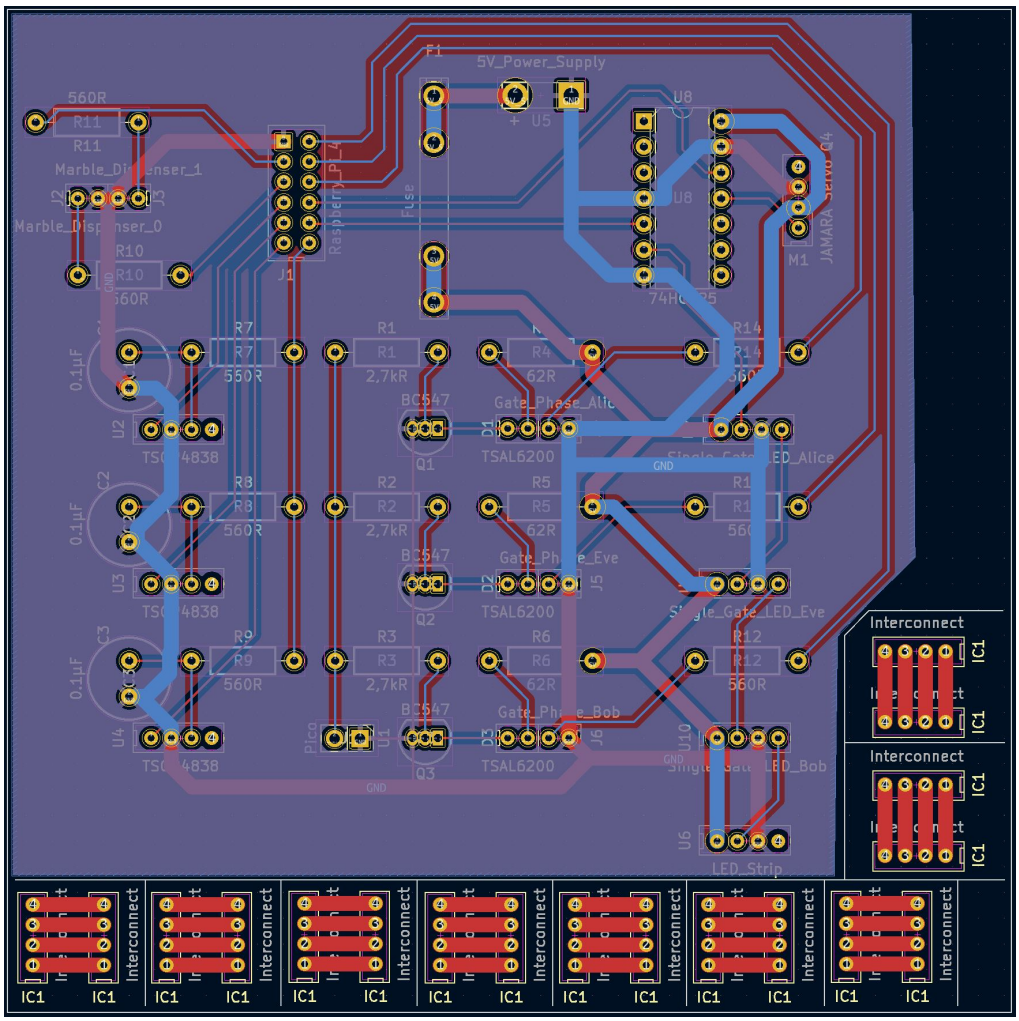

Figure 5.8.: Finished circuit board from the manufacturer

5.3. 3D Design and Printing

Now with the box and outer assembly finished and the first version of the electric circuit was done, it was time to design and build the gates and the mounts for the marble track as well as the rotary dial on top of the gates and the marble dispenser. Because the author of this thesis is most familiar with the 3D software "Blender", all designs were made in Blender. An argument could be made, that a true parametric CAD software might have been better suited, but since this would have prolonged the design process by quite a bit, while the author learns a new tool, Blender seemed like the more reasonable choice.

All 3D printing, except one later iteration of the rotary dial, was done on a Prusa i3 MK3S+ 3D printer [3]. This printer was one of two PLA printers available institute. The other being the newer Prusa MINI+ [4] which was almost always in use and hence couldn't

[3] https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/
[4] https://www.prusa3d.com/category/original-prusa-mini/

be reliably utilized by this project. The PLA used was a standard 1.75 mm filament from various manufacturers and differing colors, depending on what was currently loaded into the printer at the time of use. Since no special demands had to be met by the 3D print (like being especially durable, flexible or rigid) any standard filament would be acceptable. The 3D-printing workflow involved exporting the design files from Blender to the .stl file format, then importing them into the Prusa Slicer software which had predefined settings for the printer and was used to generate the .gcode files needed for the printer. Except for changing the preset print settings from 0.2 mm quality to 0.15 mm quality for better results with tight margins all the defaults were kept. Supports were only used for the sliding buttons in the marble dispenser (see section 5.3.3). After both the 3D view and the sliced view were checked for faults, the .gcode was exported to an SD card which the 3D-printer used to file storage. From there the print could be initiated.

5.3.1. Rotary Dial

One of the longest and most difficult designs was the rotary dial which sits on top of the gates and lets the users chose their measurement base. With this dial being the only haptic interaction that the user on Bob's end will have with the system and one of two haptic interactions the user on Alice's end has, it was immediately clear that this dial had to be able to clearly convey the concept of the orthogonal and diagonal measurement bases while providing excellent feedback to the user.

Since the two bases are only rotated by 45° this is also the maximum this dial should rotate. So the search for any readily available solutions began, but ended without any meaningful find. While there are setups that allow for eight different states, with each state 45° rotated to the other, such solutions came in very large sizes, since they had to accommodate eight outputs. Additionally the original plan for the electronics only included a Raspberry Pi (see section **??** for more details), the dial had to put out a binary signal, as the Raspberry Pi is incapable of measuring analog input directly.

5.3.1.1. Version One

Thanks to all these limitations and constraints the decision was made to design the dial from the ground up. With haptic being one of the main focuses it was important that the dial snaps into place when the correct angles are selected. Also no angles outside the needed 45° range should be select-able and at least in one of the two correct places a digital signal must be sent (the other could just be interpolated from the missing signal). All this lead to the design show in Fig. 5.9

This design was split into an upper part, shown on the left hand side in each picture of Fig. 5.9, and a lower part, shown on the right hand side in each picture of Fig. 5.9. The two parts could be stacked together and would lock in place thanks to a ridge (3) and overhang (6, barely visible) that would interlock when the two halves were completely closed. An extrusion (4) on the upper part fit into a circular cutout on the lower part which allowed for snapping into the right positions. Overshooting was prevented by two walls (2) on the lower part, which blocked the back side of the extrusion on the upper part to move past the snapping grooves.

To get a digital signal, a hole (1) was left on the lower part, which could fit a simple, electrical switch. The extrusion (4) on the upper part would then not only snap into

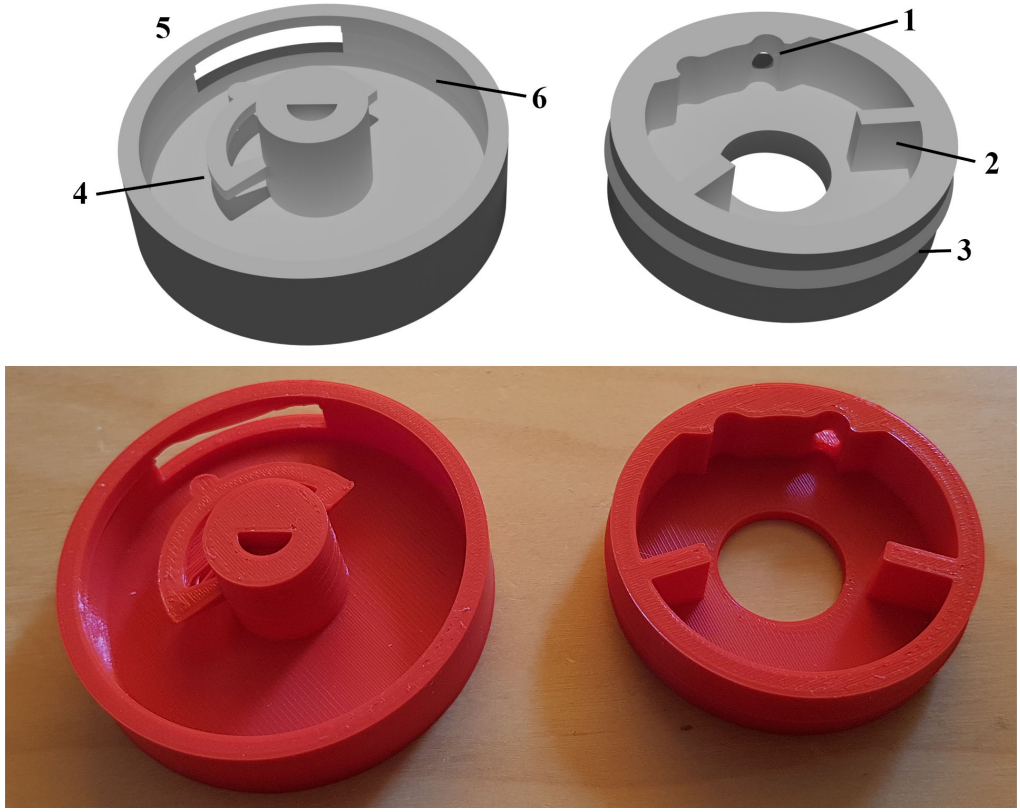

Figure 5.9.: 3D-design (top) and -print (bottom) of the rotary dial, first iteration. In each image the left part is the top part of the dial and the right is the bottom (1) switch hole; (2) limiter wall; (3) ridge; (4) extrusion; (5) cable window; (6) overhang

place into the grooves, but also trigger the button when it snapped into the right hand side groove. For the cables a cutout window (5) was placed on the upper half, which allowed the cable to come out the side even when the dial was turned.

After some tests this design was found to be faulty and unusable, mainly to the fact, that the extrusion (4) would grind down relatively fast and no longer trigger the electrical switch resulting in a non functional dial after only about ten rotations.

5.3.1.2. Version Two

To address these issues a second design was made. This time around the electronics had already advanced to a point where the Raspberry Pi alone couldn't handle it all anymore and a micro controller in the form of the Raspberry Pi Pico was added (see section **??** for more details). Due to this change in the electronics, a new dial design was possible. One with a analog rotary encoder in the form of a potentiometer. This would eliminate the need for the extrusion to trigger any signal and it could solely be used for the snapping mechanism. Instead a shaft in the center of the upper half would pass through the cavity of the potentiometer, which was mounted onto the lower half. The result of these changes can be seen in Fig. 5.10

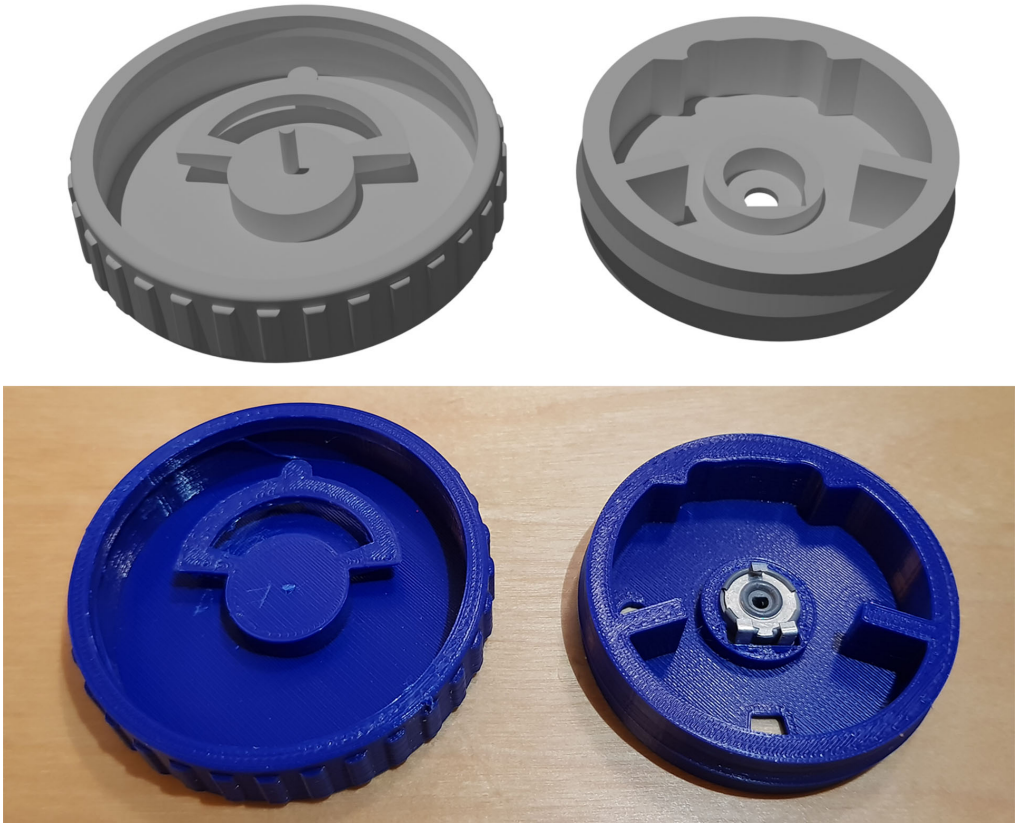

Figure 5.10.: 3D-design (top) and -print (bottom) of the rotary dial, second iteration. In each image the left part is the top part of the dial and the right is the bottom

The new version also gained a few quality of live improvements, such as the nubs around the outer shell, which improve grip and and fell nice to the touch tanks to their round edges. Also added were a pair of screw holes which match later versions of the gates (see section 5.3.2) for mounting. But most important of all is the mold for the potentiometer. The 3D-printed version shows the bottom half with an added potentiometer, however the keen observer might immediately spot a key difference between the 3D-design and the 3D-printed version of this dial: the shaft, which should turn the potentiometer, is missing from the 3D-printed part. It turned out that printing the shaft vertically made it rather unstable and it would twist off after one or two turns of the dial. Even reprints with a slightly larger shaft were not able to withstand the torque that the potentiometer required for turning.

This proved to be a fatal flaw of this iteration and another redesign was required.

5.3.1.3. Version Three

After multiple tries to improve the strength of the printed shaft in version two, it was decided that the shaft had to redesigned completely. Since the most detrimental issue with the version two shaft was that the 3D-printer would not perfectly align all layers on top of each other on such a small and very bendable area, the solution was to print the

shaft horizontally instead.

By carving out the shaft and printing it as it's own part, the process was able to take full advantage of the fact, that layers printed horizontally directly on the bed of the 3D-printer are usually the strongest and most durable layers of the entire print. Of course this meant that the top part also needed some sort of receptacle for the new part. With the previous experience of twisting off a part that was too small, the receptacle was scaled to a size which ensure that this would not happen again.

One more flaw that was found in version two, was that with the now completely solid top part, the two halves would no longer fit properly together. Thanks to the improved rigidness of the top part, it would no longer bend when putting the two halves together, which meant that it would no longer glide over the ridge of the bottom part. To address this issue a very simple solution was applied: reducing the rigidness of the top part by adding a small wedge across the outer wall and along most of the outer part. Everything put together is shown in Fig. 5.11

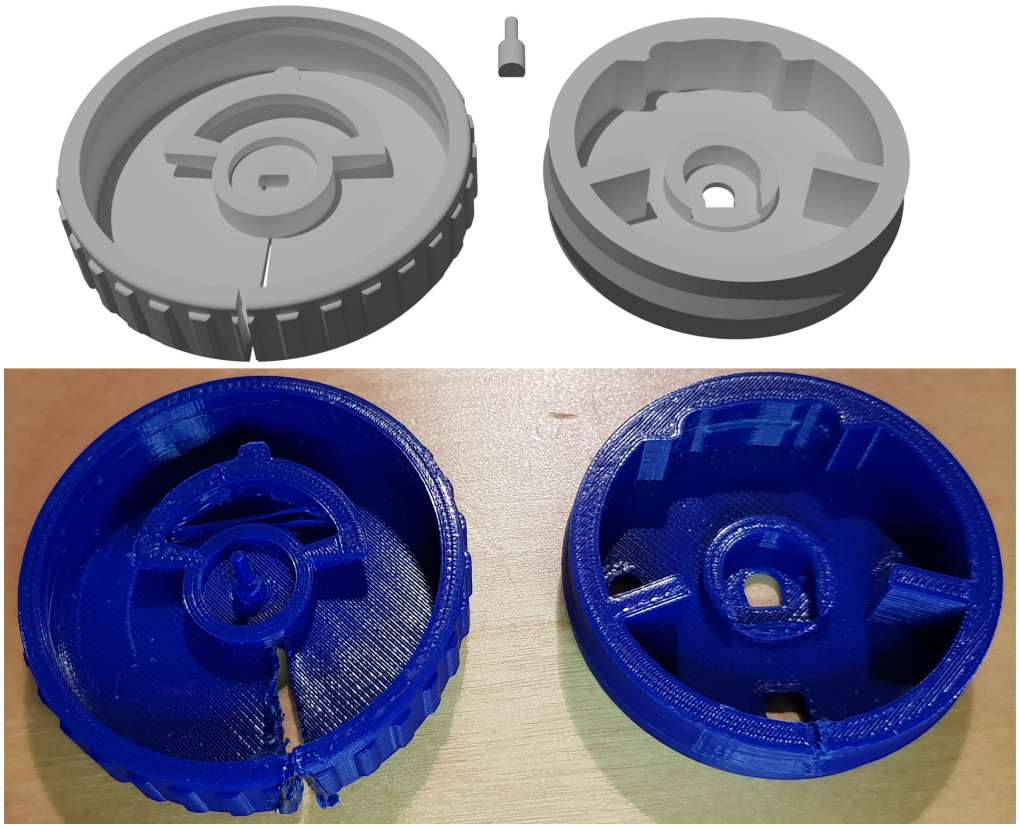

Figure 5.11.: 3D-design (top) and -print (bottom) of the rotary dial, third iteration. In each image the left part is the top part of the dial and the right is the bottom

Some more quality of live improvements were also added, which made it easier to access the connectors on the front of the potentiometer. To allow for more space between the to half and the cables connected to the potentiometer, the part in which the shaft resides was also hollowed out some. With these changes the design of the dial was finalized and utilized in the completed prototype, although putting the two halves together was now

rather challenging, since the orientation of the top half had to match the direction of the potentiometer almost perfectly. But in all three attempts this worked on the first try and none of the shafts broke off.

5.3.2. Gates

Compared to the rotary dial the gates went through far fewer design iterations. Their main purpose were to provide a visual indicator of the space which each participant can call their own. So Alice's space ends at her gate and when the marble passes her gate it leaves her sphere of influence. To enforce this idea the gates of Alice and Bob were put on the very edges of their box, right up against the divider walls.

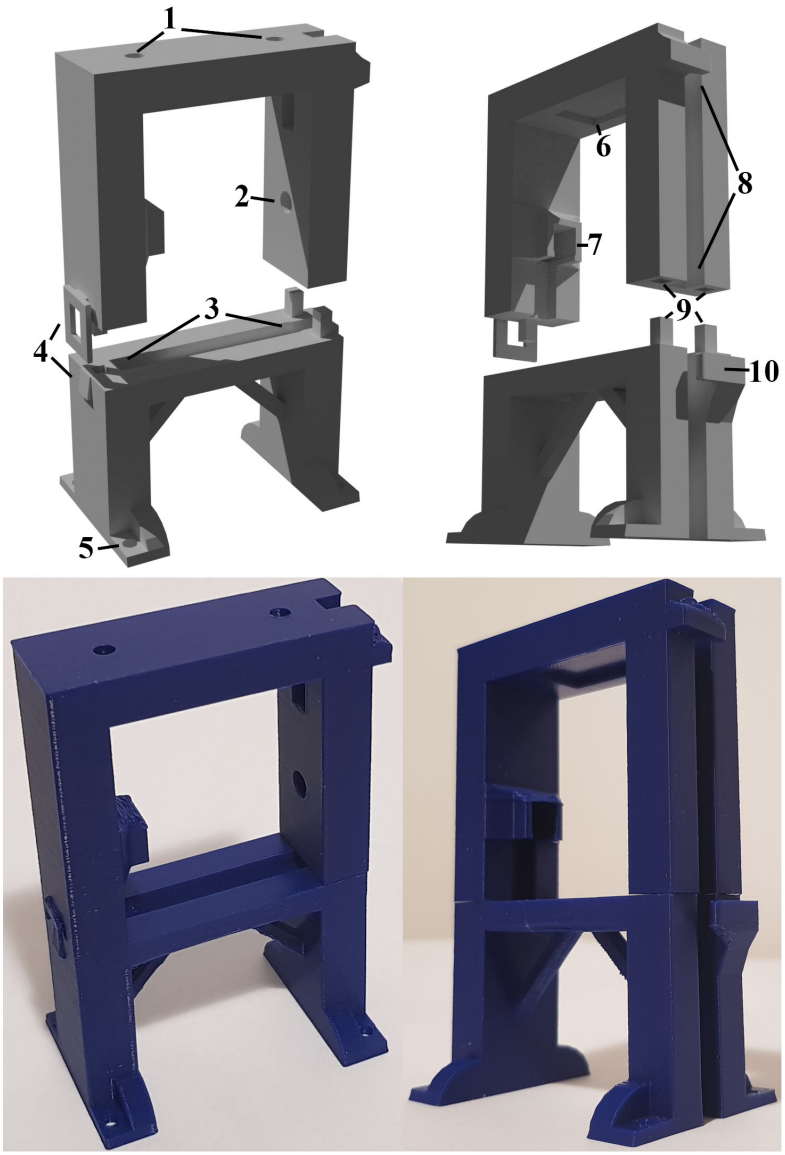

Figure 5.12.: 3D-design (top) and -print (bottom) of gates.
(1) dial mounts; (2) IR LED mount; (3) cable guide; (4) clip and latch; (5) screw holes; (6) colored LED inset; (7) IR sensor mount; (8) cable guides; (9) mounting holes and stands; (10) cable clip

As for the design of the gates themselves, they are also split in a top and bottom half. The original idea was that this allows for Eve's gate to be physically removed when it's

not in use without removing the screwed on bottom part. This however proved to be an invaluable design decision for other reasons as well. For example the fact that the marble track - which runs through the gates - would prevent the installation or removal of any components beneath the track, once completely installed itself. But thanks to their two part design the upper part of the gates, which houses all of the electronics, can be still be removed in such a case, which allowed for much easier maintenance of the installed electronics.

Fig. 5.12 shows the various electronics and mechanical components housed by the gates. On the very top are the two screw holes (1) that the rotary dial screws into. Directly beneath sits the RGB LED (6) which indicates the currently chosen polarization base by shining either green or red light, when the rotary dial is turned. Further down is the mounting hole for the infrared LED (2) which goes all the way through to the other side where the cables are housed (8). Opposite the IR LED sits the infrared sensor (7). The two of them compose the light barrier that detects marbles rolling through the gate.

On top of housing the electrical components themselves, the gate were also designed with cable management in mind, which is why they contain designated cable guides for both the IR sensor (3) and the LEDs (8). These guides are complemented by two cable clips, one half way up (10) and the other at the very top.

To improve stability and make it easier to join the two halves together, both sides of the gate are equipped with mounting holes and stands (9) which fit into each other. This is also the only part that was re-designed. The original concept for the gates had more, but smaller holes and stands, which made it more resilient against rotations, but weakened the over all stability of the stands themselves. This lead to them breaking offs on a regular basis, when a gate was assembled and disassembled multiple times. In the final design the stands were reduced to just three, but these were much thicker than before. This gives them the needed strength to withstand multiple dis- and re-assemblies.

In the testing phase it was discovered that the IR LEDs were too bright and the sensors would pick up signals from reelections, even when a marble broke the direct line of sight. This was helped a bit by switching from clear marbles to solid metal ones, but ultimately some aluminum foil had to be taped over both the IR LEDs and the receiver to weaken the signal and narrow the detection angle.

5.3.3. Marble Dispenser

The most intricate design of all the 3D-printed parts was the marble dispenser. It had to not only release one marble at a time but also redirect the marbles left and right, depending on which button was used to release a marble and signal the electronics that a marble hat been release and to which side it went. After trying a few different designs, which included a rotary release mechanism, it became clear that a push release would be the most usable design for multiple reasons. For one it has a very clearly defined point of release and a satisfying user feedback, when a marble is release. On top of that the design with two push buttons is very intuitive and leaves little room far ambiguity, on how the mechanism is used.

The marble reservoir (1) holds all marbles and funnels them into the single marble chute beneath it (2). The insides of the reservoir are angled towards a single hole in the bottom which is has an only slightly larger radius than a marble itself. This ensures that only a single marble is able to get into the marble chute. The capacity of the reservoir is

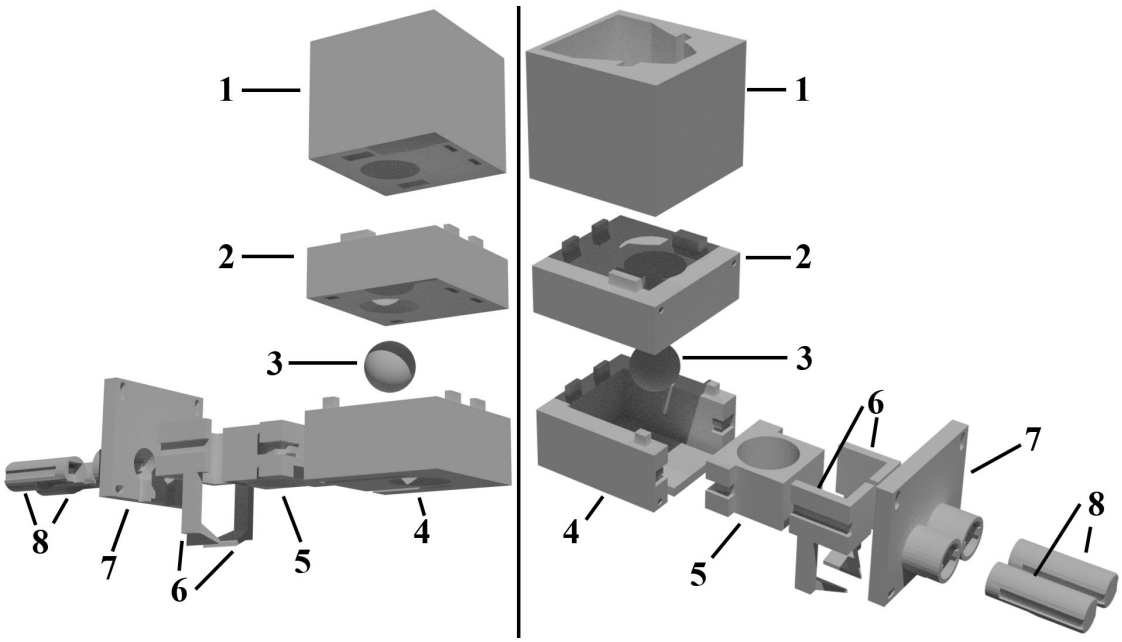

Figure 5.13.: 3D-design exploded view of the marble dispenser.
(1) marble reservoir; (2) single marble chute; (3) marble for scale; (4) base; (5) release sled; (6) side pushers; (7) front panel; (8) buttons

10 marbles. For a marble to be released it needs to fall from the chute into the release sled (5), which can then be pushed inwards by either one of the two side pushers (6) to align the sled with the release hole in the base (4). Through this hole the marble is then released and pushed to one side by the slopes, which are attached to both pushers. The sled then returns to it's position beneath the chute and accepts another marble.

The automatic push back is accomplished by two rubber bands that attach to the small hook on the back of the sled and another two hooks on the front sides of the base. Grooves on the sides of both the base and the sled provide a guide for the rubber bands and prevents them from getting caught on anything while the sled moves back and forth.

Since with each marble release only one of the two side pushers should move forward, they also get their individual rubber bands which hold them back. These bands are attached to small hooks on the front panel (7). The two buttons (8) are there to actually push the entire assembly inwards. They also provide the electrical signal for when a marble is release through a small electrical switch, which is inserted into each button and is the sole contact point between the buttons and the pushers.

The buttons are held in place by a small grove which goes not quite all the way along the sides. This allows them to slide on an inner guide, which is build into the front plate, but prevents them from falling out. Wires, which connect the electrical switches on each button with the rest of the electronics, can pass through small holes on the bottom of the front plate and the hollowed out structure of the buttons allows for a small cable reservoir, which allows for free forward movement of the switches inside the assembly.

Fig. 5.14 shows the assembled version of the dispenser, both in 3D and printed. This figure shows even more clearly the two cutouts on the base through which the slopes, which are attached to the pushers, can glide in order to position themselves beneath the

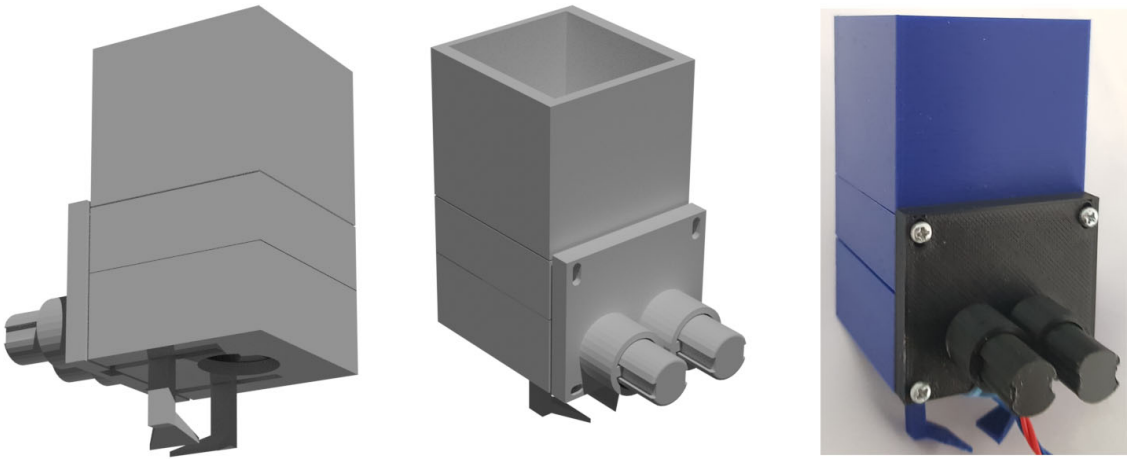

Figure 5.14.: 3D-design and -print of the assembled marble dispenser.

hole in the base, when a marble is released. Also visible are the screws which hold all parts, except for the marble reservoir together and which give the entire assembly a stable feeling.

For clarity the installed version of the dispenser has glued on labels for which button is 0 and which is 1. The difference in color is simply due to the fact, that the first print of the front panel and the buttons failed, because the adhesion of the buttons to the printing plate was too low, which caused them to topple over, which in turn caused PLA to go everywhere and destroy the original prints. When re-printing these parts the blue PLA was in use and only black was available but the properties of the material are the same. The groves on the re-printed buttons had to be smoothed out by hand a little bit, since the now utilized supports left a few rough spots, that caused the buttons to get caught on the guides of the front plate.

5.4. Marble Track

In order to add one more material, which is not plastic, the marble tack was chosen to be made from steel wire, held together with solder. Steel was not only chosen for how it looks but also because it represents a malleable material which allowed for small deviations in the 3D-prints to be corrected by simply adjusting the hand made steel constructs. Due to the nature of the track being hand made, a lot of the work was done by approximation and fine adjustments until the desired result was achieved.

In order to first test if steel and solder would be able to provide the necessary strength to hold not only the marble track itself, but also the dispenser, a small track was created at the beginning of the project. This track can be seen in Fig. 5.15. The distance between the two lines of the track was chosen to be around 75% of the diameter of the marble, which allowed it to roll smoothly but securely guided on the track. To keep the distance consistent along long stretches of track, small half rings in the correct size were made and soldered to the track in regular intervals. For these to actually be consistent in size a template was needed. Coincidentally the author of this paper had a strong metal rod at home which happened to have the exact dimensions needed that the steel wire could

Figure 5.15.: A test track made with steel wire and solder

be wrapped around to achieve the necessary radius.

For longer parts of the track a method was needed to create a straight segment from the coiled steel wire. The solution here was to cut off a piece of coiled wire, attach one end to a strong object - again a use for the aforementioned metal rod - and put the other end into an electrical drill, like you would a drill bit. Then the drill was turned on while the entire wire was kept under tension. The torsion of the drill combined with the applied tension straightened out the coiled wire with ease.

Bending the track coherently was also a challenge. Here a few cylindrical objects were used to provide a consistent radius. The objects were simple household paraphernalia like a glass bottle, a few drinking glasses of varying sizes and a tin can. Of course all bends had to be modified by hand to fit into the setup.

Another tricky part were the two track switches at either end. Where the one on Alice's end had to merge the marbles from different directions into one, the one on Bob's end had to divide them apart again. One such switch is show in Fig. 5.16.

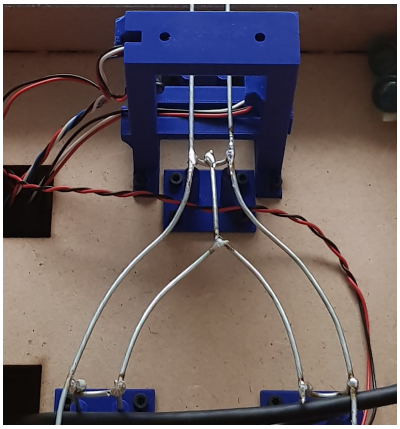

Figure 5.16.: A track switch

It took quite some work and collection of empirical data to get the transition from rolling on two rails, to one rail and the support, back to two rails again running smoothly. A surprisingly large role played the exact curvature of the center support. If it curves off too quickly, then the marble will be too low and hit the second rail at the end of the switch at and angle which wont allow it to rise up to the base level again. This causes the marble to get stuck at that point. however when the curve off

was not quick enough, then the marble would lose
too much momentum on the support and get stuck at the beginning of the switch. Only after carefully adjusting the curve of the support, was a consistent result achieved.

5.4.1. LED Strip

One more feature of the track is a secondary track of LEDs running beneath it. The idea behind this LED strip is to provide a light source which moves in sync with the marble to reinforce the metaphor of the marble representing a photon. As with the marble track, the LED strip had to be split into five parts: two for each side of Alice and Bob and one for the center line connecting the two, going through Eve's gate.

While the center line could just be one coherent LED strip, the parts following the curves on either end needed to be individually placed to properly match the track above. To more easily place them, a cardboard cutout of the curved parts of the track were created and the pieces of the LED strip glued to. afterwards the pieces were soldered back together with the use of silver wire in the correct length.

5.5. Software

At the hart of the user experience lies the graphical user interface (GUI) with its UI/UX design. Because it plays such a key role, a lot of effort was put into its design, both to keep it as simple and minimalist as possible and to guide the user without overwhelming them. Of course the GUI can only provide such an experience if all other interactions with the prototype are also reactive and robust. To achieve this the application runs highly multi-threaded with three concurrent threads at all times and additional threads spawned by certain events.

5.5.1. Software Choice

To begin with a choice had to be made which programming language was to be used and while the author of this thesis sees Java as his best language, the choice ultimately fell on Python. Python was chosen because of its vast library on the Raspberry Pi and the ability to easily interface with the GPIO system.

5.5.2. Hardware Controller

Now that the language was decided on, a few more libraries were needed to complete the task at hand. First was the library to program the programmable LEDs. As these are very standard LEDs in this regard, the rpi_ws281x library could be used to address them. With this library offering a simple API to address each LED along the strip the author build a class in Python which provided all necessary methods for the operation of the prototype. Most notably the method to flash any given part of the strip, which is used every time a marble is release to flash the LEDs under the marble while it travels along the track.

Since this class now handled all matters regarding the LEDs, it had to be very responsive and couldn't lock up the main thread while it waited for the marble to move forward. Because the author of this thesis is very familiar with game programming,

it came naturally to leverage these skills, as games also have responsiveness as one of their top priorities. So the decision was made to put the LED class (or rather the object spawned from it) on a frame interval with 100 frames per second (FPS) being the target. All new commands would then be added in a thread save manner to a locking queue (with deadlock prevention). The thread then completes all tasks in the queue every frame and sleeps for the remaining time. Remaining time being calculated as $\frac{1}{100}$ − (time needed to complete the tasks). The same responsiveness was needed for the servo motor, so now with this task already solved for the LEDs the same code was simply reused to also put the servo controller on a FPS based thread.

5.5.3. UI/UX

With the hardware controller done and responding quickly to user input the only thing remaining was the UI. As mentioned before a minimalist style was important. That's why the choice fell on the customtkinter library. This library aims to replace the widely used tkinter library by providing the same utilities but with a modern and minimalist look. To go into every class involved in building the GUI would be too extensive for this thesis. Therefore the best way to demonstrate it, is to actually show it. Following is a gallery of images, how the GUI looks like on the screen in front of Alice. Bob's screen will show almost the same design, expect that the "Sent" string is replaced by a "Measured" string, since he only measures photons on his end. As a side note: the "button1" button is a placeholder for an unfinished options menu, which was planned to give users the option to automate gates, so that they automatically select a new setting after each marble passed through. Unfortunately time constraints prevented the completion of this menu.

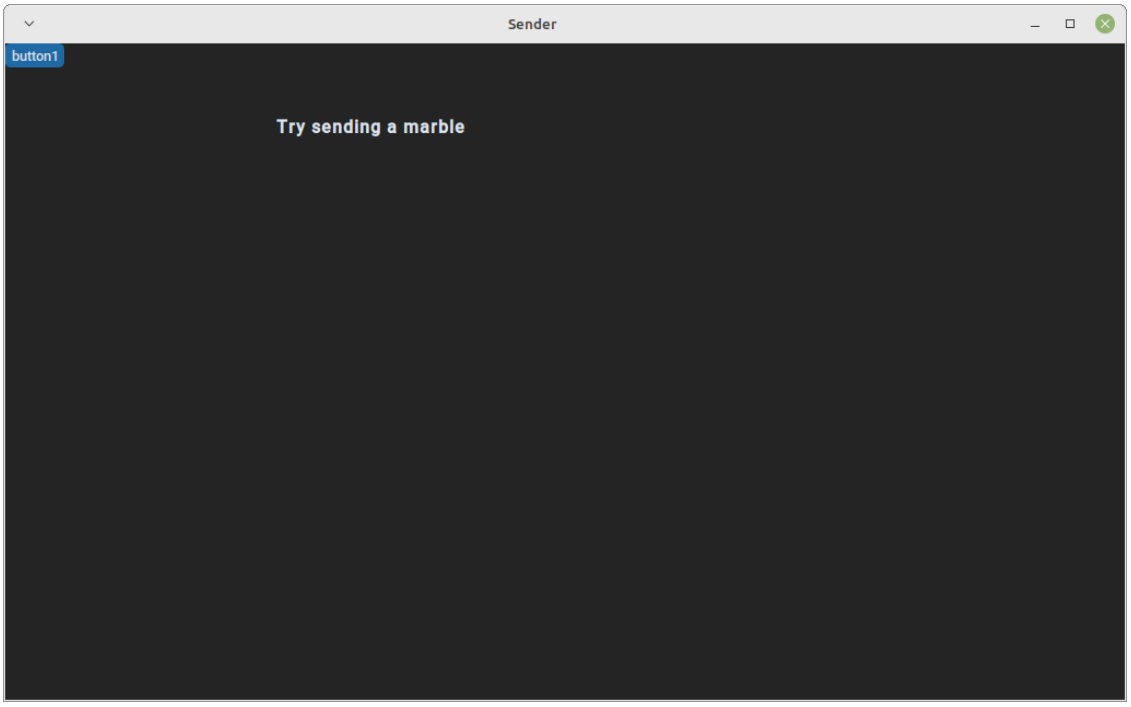

Figure 5.17.: The GUI right after starting the UI

Figure 5.17 shows the starting screen. Since nothing has happened yet it requests that the users send a marble through the physical buttons.

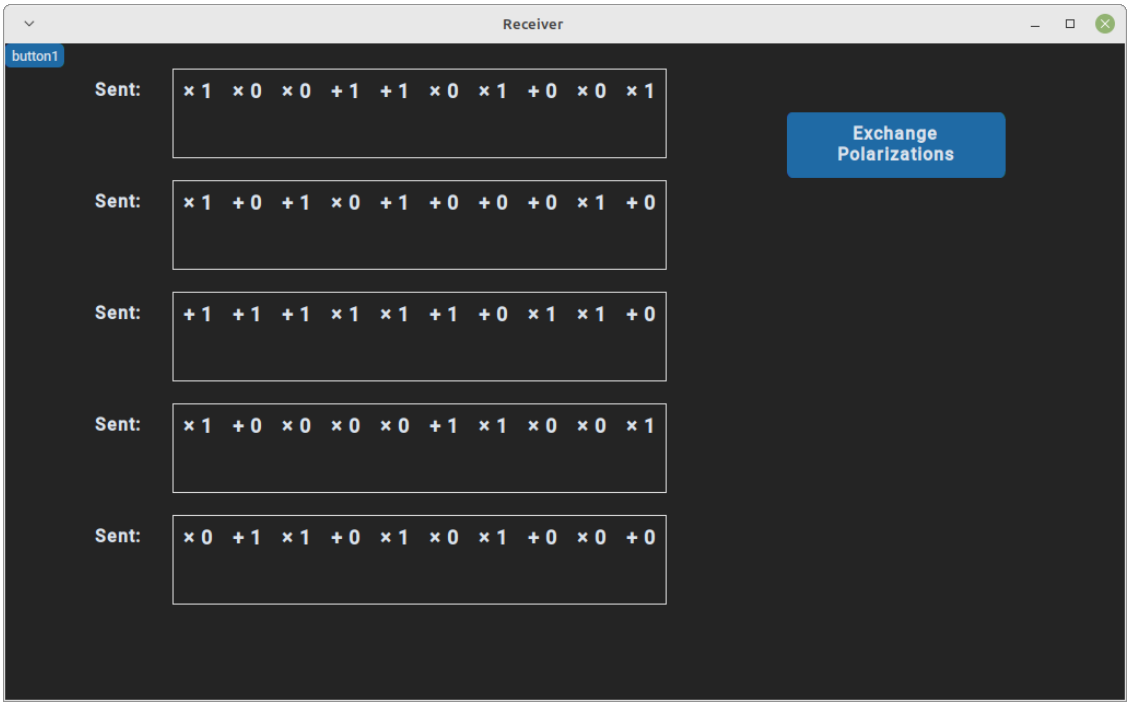

Figure 5.18.: The GUI after sending 50 photons

Figure 5.18 shows the screen after Alice has sent 50 photons. It shows in the center a list of all her sent photons with both the chosen polarization base and the corresponding 0 or 1. This list is variable and only ever shows as many lines as minimally needed. The button to the side for exchanging the polarizations with Bob appears after the first photon is sent and can be pressed at any time to move to the next phase.

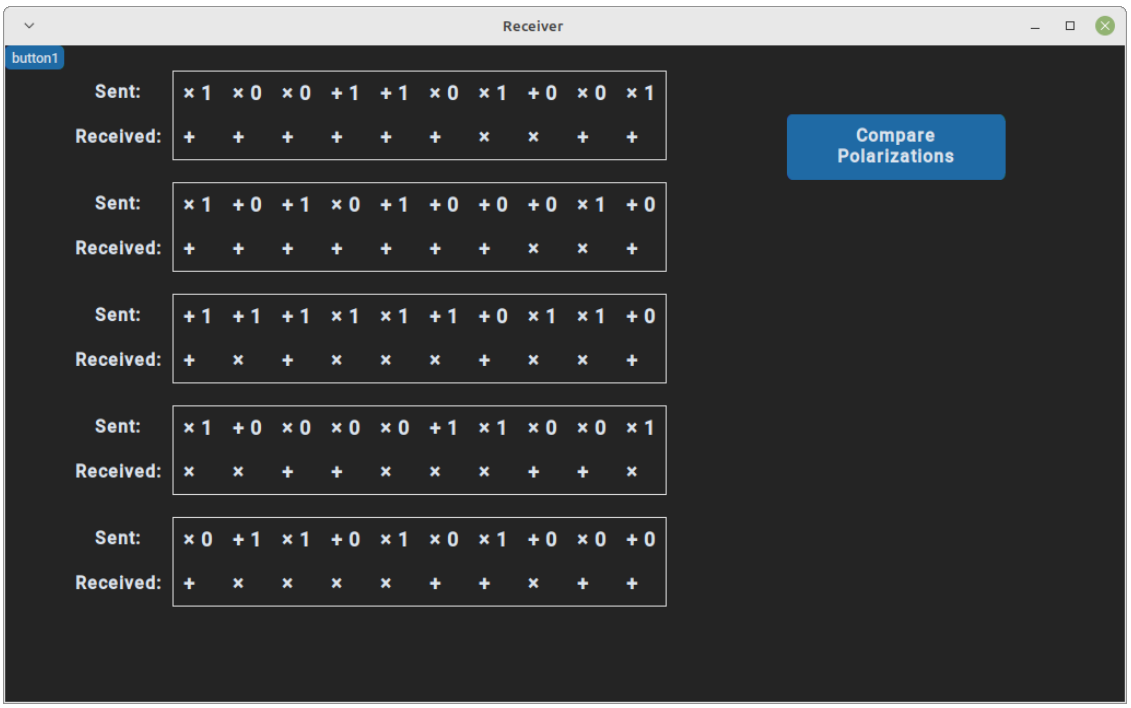

Figure 5.19.: The GUI after exchanging polarizations

In Figure 5.19 Alice has now exchanged her polarizations with Bob. She now sees his polarizations on her screen and he sees hers on his. The revealing of the received polarizations is animated and happens in succession. The button was replaced with a comparison button. Pressing it will start an automated process of comparing which bases match and witch differ. This process can also be done by hand by simply touching all photons with matching bases, but the comparison button does not yet respect the users choice (even though this choice will be displayed in the GUI). The time constraint on the thesis prevented this feature from being fleshed out more. Also, as will be shown in the user study, it would go contrary to what the users wish for.

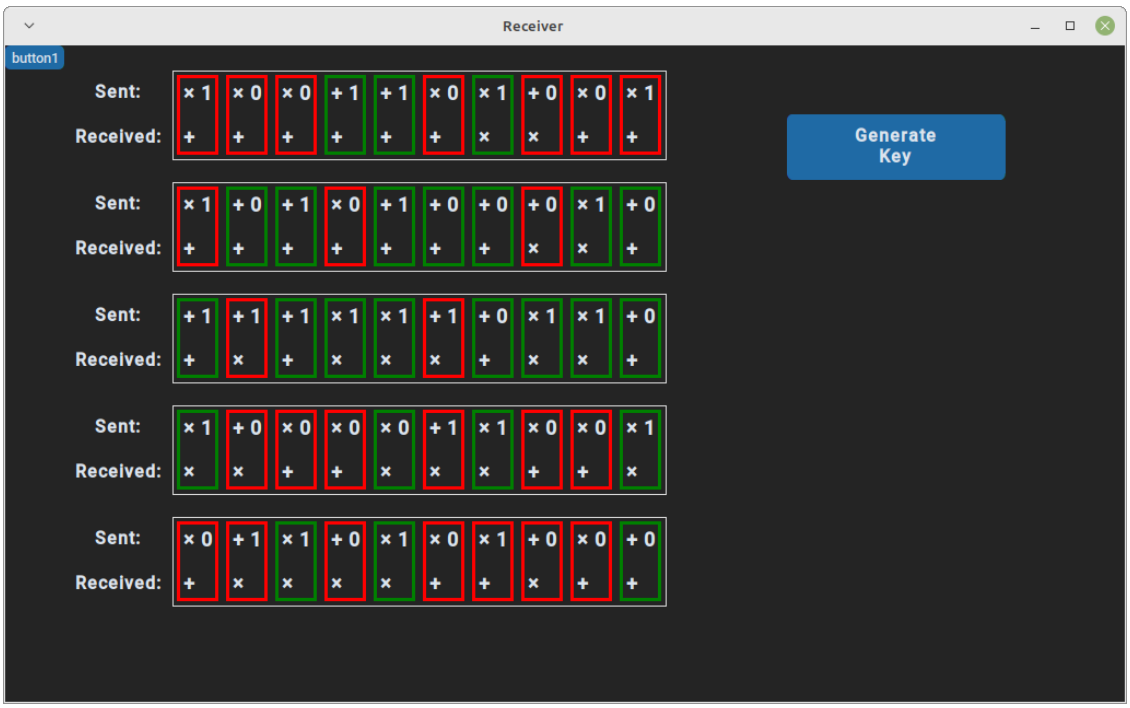

Figure 5.20.: The GUI after exchanging polarizations

Figure 5.20 shows the completely compared bases. This process is again animated. Equal bases are highlighted in green, differing in red. The button changed a final time, now offering to generate a key.

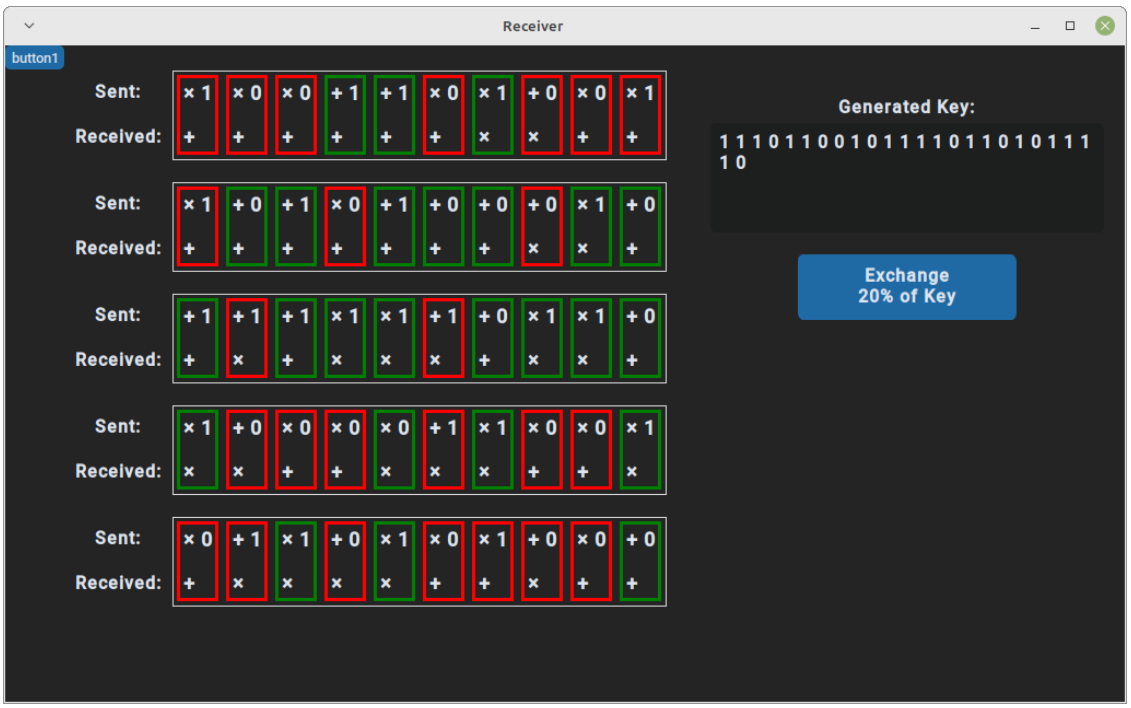

Figure 5.21.: The GUI after exchanging polarizations

The generated key can be seen in Figure 5.21. The generation algorithm simply takes all binary data from matching bases and disregards differing bases. The final step of the algorithm can be initiated by pressing the new exchange key button. Here 20% were chosen due to the usually pretty short keys. The actual algorithm would usually only exchange 10%, but that could lead to only very few bits being exchanged.

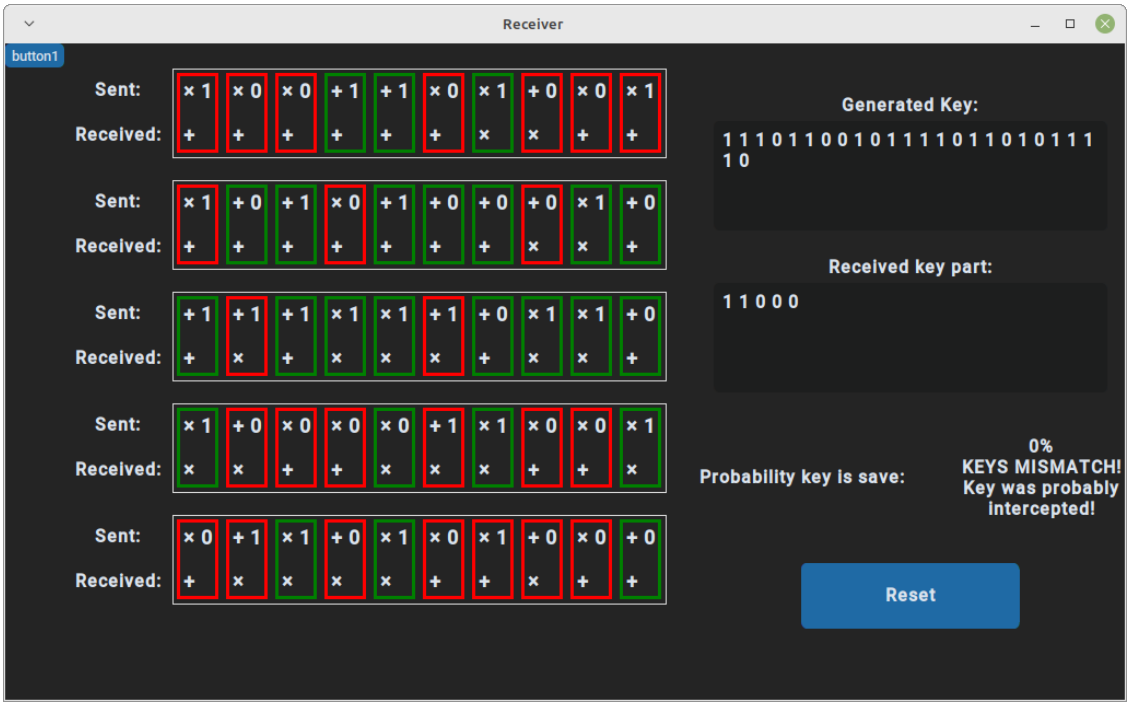

Figure 5.22.: The GUI after exchanging polarizations

Figure 5.22 shows the reveal. In this case some parts of the exchanged key didn't match, which indicates that Eve was active and intercepted the key. If no mismatches are found, the message would instead the actual probability calculated from $0.5^{\text{number of exchanged bits}}$. The option to start over is displayed.

5.6. Finished Prototype

With all the different parts together the final prototype is ready for user testing.

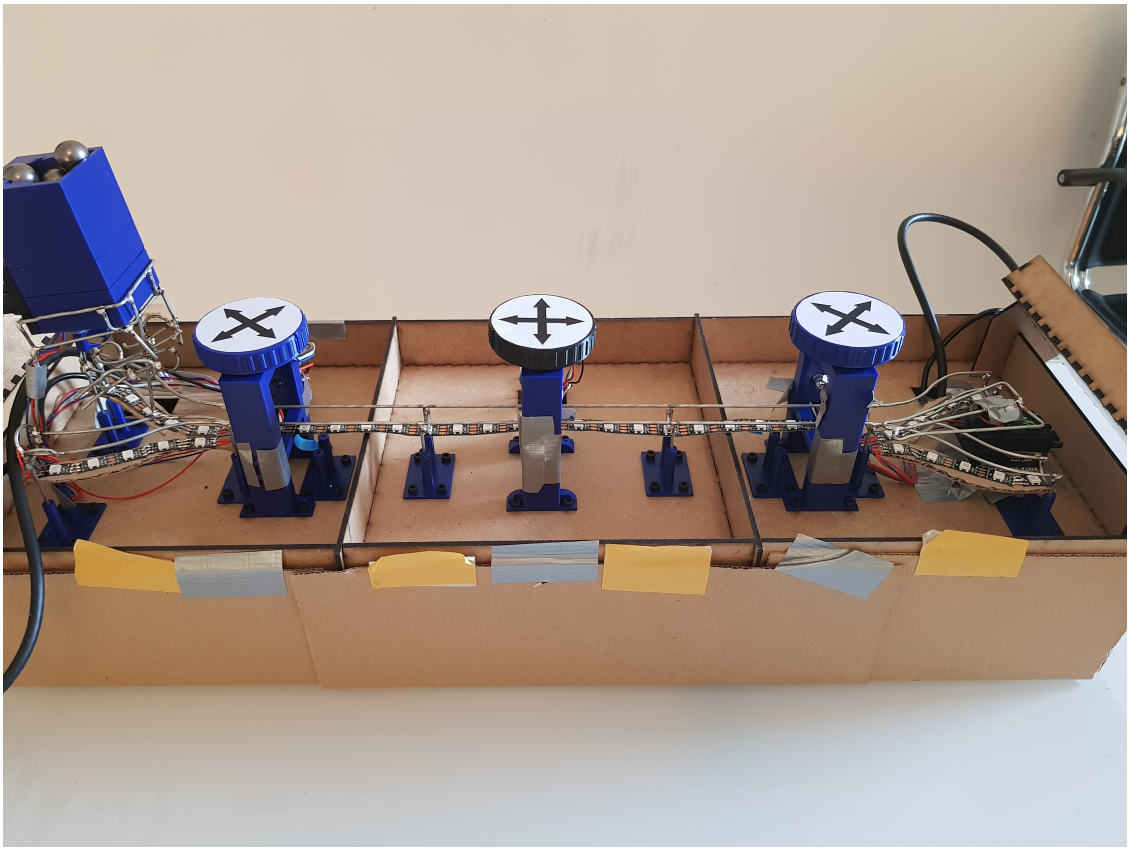

Figure 5.23.: The finished prototype

6. User Study

Since time was scarce towards the end of this thesis, only a qualitative user study was performed and not a quantitative one. To get some feedback on how well received the prototype is, it was shown to three participants, one after the other and feedback from the previous participant was used to improve the demonstration for the next. All participants had no background in cryptography and none knew anything about the BB84 algorithm. Two participants are physicists and had a general understanding of quantum mechanics.

6.1. Procedure

All three runs of the study were done following the same procedure, with only the explanatory script of the author being adjusted after each participant:

- Participants started out as Alice and performed one exchange of ten photons as her and then following completion of the key exchange, before switching to Bob.
- For each screen the author explained to the participant what actions the current step entailed, why they needed to be performed and what should be expected.
- After completing one run of the key exchange as Alice users were asked how well they rated their understanding of the proceedings as well as how the prototype performed
- When both runs were completed a detailed feedback was requested and noted

6.2. Feedback

6.2.1. First Participant

The first participant didn't understand the working of the BB84 algorithm at all after completing the study. They indicated that the lack of a well presented script on the authors part was manly to blame and that with a better introduction to each step they might have understood it. The author then spend some time explaining the algorithm in detail, until it was completely understood by the participant. Following this discussion the participant pointed out a few key points that were missing in the presentation, which prevented them from understanding. The points were:

- The motivation for why a key exchange is needed in the first place was missing
- The explanation of why current Diffie-Hellman wont be resistant to quantum computers was confusing. It was suggested to not motion Diffie-Hellman at all and just focus on explaining in layman's terms what the basics of cryptography are
- The concept of the polarization bases was poorly explained and should make more mention of that it's simply a measurement basis which either guarantees a result, or gives an even likelihood of either outcome.

On the positive side they highlighted how nice the prototype felt to use, with the haptic being what they would expect from such a system. While on Alice's end they encountered no issues with the performance of the system at all. On Bob's end it was found that the servo motor could sometimes be too slow for a fast moving marble and hit it in a way that prevented the marble from completing it's journey.

6.2.2. Second Participant

Having learned from the first one, that the script needed improvement and simplification, the second participant was presented with a more detailed description of every step by the author. This resulted in an overall better understanding of the algorithm after the completion of the study, even if some points still needed clarification afterwards. The key points that participant two highlighted for improvements were:

- Again the concept of the measurement bases was poorly understood. This time the participant had a background which allowed him to understand how quantum mechanic measurements were taken and was confused by the basis representing to orthogonal states that could not be measured at the same time.
- The concept of Eve and how she influences the results was not explained well enough

Overall the participant enjoyed the interaction with the prototype and agreed that they now had a better understanding.

6.2.3. Third Participant

Further adapting the script to make the measurement bases more easily understood helped with this participant immensely. After finishing the run they claimed to have understood the algorithm and showed a basic level of understanding after being questioned by the author. The remaining key issues were more of a usability type:

- Marble blockages on Bob's side need to be addressed
- The marble dispenser could sit more securely
- "Phantom" photons can accrue, if something breaks one of the IR light grids unexpectedly

Overall the participant enjoyed the interaction with the prototype and it was discussed if the third issue was not actually a feature, since this could happen in a real world application.

7. Conclusion

Overall the goals that were set could be completed satisfactorily. The prototype presents a working machine that can be used to explain the BB84 algorithm even to laymen. It is not perfectly working and has a few issues, but that was to be expected of a prototype.

The main issues which should be improved in the next iterations are:

- Presenter needs a detailed script on how the participants should use the prototype
- Software needs completion in form of a settings menu
- Software needs completion in form of a working Eve
- Auto-fill of the software should also change the gate color and send "photons" on the LED strip
- Servo needs to be faster, either by increasing the distance between it and the gate, or by compensating and moving it before the marble reaches the gate, simply through timings
- Box needs a proper base instead of cardboard
- It would be good to redo the electronics with the new insights gained from the prototype - namely removing unnecessary parts from the board and integrating the Pi Pico better
- Gates should be made bigger (about a factor of 1.5) and the cable guides should include more hooks. Maybe the cables could be completely hidden away
- Raspberry Pi settings should automatically load on power up (right now ./initial_-config.sh must be executed manually)
- GUI should launch automatically on power up (right now the Raspberry_Pi_-Master.py program needs to be launched manually and with sudo)

With these recommendations the prototype should be regarded as a resounding success.

A. Appendix

A.1. Electronics

A.1.1. BOM Circuit Version One

A.1.2. BOM Circuit Version Two

#	Part number	Description
1	KES 1	Kaltgerätestecker horizontaler Flansch
1	WIPPE 1552.3102	Wippschalter, 2x Aus, schwarz, I-O
1	GLP GPV-60-5	LED-Netzteil, 40 W, 5 V DC, 8 A, IP67
10	VI MBB02070C6809	Dünnschichtwiderstand, axial, 0,6 W, 68 Ohm, 1%
10	VI MBB02070C2200	Dünnschichtwiderstand, axial, 0,6 W, 220 Ohm, 1%
15	VI MBB02070C5600	Dünnschichtwiderstand, axial, 0,6 W, 560 Ohm, 1%
10	VI MBB02070C2701	Dünnschichtwiderstand, axial, 0,6 W, 2,7 kOhm, 1%
10	VI MBB02070C4701	Dünnschichtwiderstand, axial, 0,6 W, 4,7 kOhm, 1%
10	SM 0,1/63RAD	Subminiatur-Elko, radial, 100 nF, 63 V, RM 1,5, 85°C, 1000h, 20%
10	KERKO 100N	Keramik-Kondensator, 100 nF, -20...+80 %, Y5V, 50/100 V, RM 5
10	BC 547B DIO	Bipolartransistor, NPN, 45V, 0,1A, 0,5W, TO-92
4	TSOP 4838	IR-Empfänger-Module, 38kHz, 90°, Side-View
6	TSAL6200	Infrarot-Diode, GaAlAs, 940 nm, 34°, 5 mm, T-1 3/4
2	74HC 125	BUS Puffer, 3-State, 2 ... 6 V, DIL-14
96	JST PH CKS	JST - Crimpkontakt, Buchse - PH
24	JST PH4P BU	JST - Buchsengehäuse, 1x4-polig - PH
24	JST PH4P ST	JST - Stiftleiste, gerade, 1x4-polig - PH
24	JST PHD CKS	JST - Crimpkontakt, Buchse - PHD
2	JST PHD 2X6P ST	JST - Stiftleiste, gerade, 2x6-polig - PHD
2	JST PHD 2X6P BU	JST - Buchsengehäuse, 2x6-polig - PHD
4	SL 1X32G 2,00	32pol.-Stiftleiste, gerade, RM 2,00
4	SPL 32	Buchsenleiste, 32-polig, einreihig, RM 2,54, gerade
4	MPE 094-1-010	Buchsenleisten 2,54 mm, 1X10, gerade
6	TASTER 3301	Kurzhubtaster 6x6mm, Höhe: 4,3mm, 12V, vertikal
4	TASTER 9302	Kurzhubtaster 6x6mm, Höhe: 5,0mm, 12V, vertikal
2	SL 1X36G 2,54	36pol. Stiftleiste, gerade, RM 2,54
1	VT-5322 W	Sync- und Ladekabel, USB A auf USB C
1	GOOBAY 55474	Daten- und Ladekabel C Stecker auf USB Mini B
2	GOOBAY 53781	High Speed Micro HDMI Kabel mit Ethernet

Table A.1.: Bill of materials for the first design

#	Part number	Description
1	RASP PI PICO	Raspberry Pi Pico, RP2040, Cortex-M0+, microUSB
1	JAMARA 033217	Servo Q4 Standard
3	LITT 04450001N	Sicherungshalter für 5 x 20 mm, 10 A
3	ESKA 520.626	Feinsicherung 5x20mm, flink (f), 8A
1	GC 2510-MB003	USB 2.0 Kabel, A Stecker auf Micro B Stecker

Table A.2.: Bill of materials for the first design

List of Figures

List of Tables

Bibliography

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[2] L. Stetter, "Supporting the understanding of quantum key distribution through tangible user interfaces," 2022.

[3] M. Swayne, "Ibm's eagle – 127-qubit quantum processor – takes fligh." `https://thequantuminsider.com/2021/11/15/ibms-eagle-127-qubit-quantum-processor-takes-flight-another-step-toward-frictionless-quantum-in-2025/`, 2021.

[4] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, IEEE, 2010.

[5] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," *IACR Transactions on Symmetric Cryptology*, pp. 55–93, June 2019.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, Sept. 2009.

[7] M. Lopes and N. Sarwade, "On the performance of quantum cryptographic protocols SARG04 and KMB09," in *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, IEEE, Jan. 2015.

[8] E. U. Council, "Regulation (ec) no 12863/20 of the european parliament and of the council of 24 november 2020
council resolution on encryption
security through encryption and security despite encryption," *OJ*, vol. 13084/1/20 REV 1, 2020-11-24.

[9] J.-P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, 2017.

[10] H. K. a. Hans Delfs, *Introduction to Cryptography: Principles and Applications*. Information Security and Cryptography, Springer, 2 ed., 2007.

[11] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*. Cambridge University Press, 3 ed., 2018.

[12] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," *Physics Today*, vol. 62, pp. 76–77, Feb. 2009.

[13] O. Shaer and E. Hornecker, *Tangible User Interfaces: Past, Present and Future Directions*. 2010.

[14] P. Horowitz and W. Hill, *The Art of Electronics*. Cambridge University Press, 2006.

[15] P. Horowitz and W. Hill, *The Art of Electronics: The x Chapters*. Cambridge University Press, 2020.

[16] M. Richardson and S. Wallace, *Getting Started with Raspberry Pi*. EBSCOhost ebooks online, O'Reilly Media, 2012.

[17] H. Delfs, Hans; Knebl, *"Symmetric-key encryption". Introduction to cryptography: principles and applications*. Springer, 2007.

[18] C. Mullen, Gary; Mummert, *Finite fields and applications*. American Mathematical Society, 2007.

[19] R. W. Shirey, "Internet Security Glossary, Version 2." RFC 4949, Aug. 2007.

[20] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 1990.

[21] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[22] H. Ishii and B. Ullmer, "Tangible bits: Towards seamless interfaces between people, bits and atoms," *Conference on Human Factors in Computing Systems - Proceedings*, 09 1998.

[23] S. Hayes, T. Hogan, and K. Delaney, "Exploring the materials of tuis: A multi-method approach," in *Proceedings of the 2017 ACM Conference Companion Publication on Designing Interactive Systems*, DIS '17 Companion, (New York, NY, USA), p. 55–60, Association for Computing Machinery, 2017.

[24] M. Resnick, F. Martin, R. Berg, R. Borovoy, V. Colella, K. Kramer, and B. Silverman, "Digital manipulatives: New toys to think with," 02 1970.

[25] M. Ananny, "Supporting children's collaborative authoring: Practicing written literacy while composing oral texts," 2002.

[26] Infoskript, "Pwm." `https://infoskript.de/pwm`, 2017.